Building Defence Capabilities for Future Uncertainty

Edited by

Laurenz Fürst · Ugurhan Berkok
David Last · Odin Bartsch

NATO OTAN
Defence Education Enhancement Programme (DEEP) eAcademy

Endorsements

I am pleased to endorse *Building Defence Capabilities for Future Uncertainty* as a timely and essential contribution to the evolving discourse on defence transformation. This volume brings together leading scholars and practitioners to address the critical challenges facing small democratic nations as they modernise defence capabilities, strengthen professional military education, and foster innovation. Notably, the publication's focus on digital transformation, emerging technologies, and responsible AI integration aligns directly with our institutional roadmap for preparing leaders to command in complex, AI-enabled operational environments. The collection's emphasis on ethical resilience, critical thinking, and collaborative approaches reflects the core competencies we seek to instil in our graduates. As we advance our own digital transformation and AI integration agenda, this work provides both strategic context and practical insights that will inform our ongoing efforts to ensure that our institution—and our people—remain at the forefront of responsible innovation and regional defence leadership.

Brigadier General Alvydas Šiuparis
Commandant
Baltic Defence College

Building Defence Capability for Future Uncertainty is a timely volume from established and new scholars and practitioners who met in Stockholm in 2024 at the International Society of Military Sciences annual conference. How should small democratic countries prepare for new security challenges? The original research in this volume addresses strengthening domestic defence, modernizing military capabilities, improving professional military education, and fostering better public-private cooperation.

As an uncertain future confronts educators, defence planners, and technical staff, this collection will provoke thoughtful discussions and new approaches.

Laurenz Fürst is Chair of the Working Group on Security and Defence Policy of the International Society of Military Sciences. He works for the Austrian Ministry of Defence.

Ugurhan Berkok is Chair of the NATO Working Group on Defence Economics and Co-Chair of the Working Group on Defence Economics and Management of the International Society of Military Sciences. He teaches Economics at the Royal Military College of Canada and Queen's University, Kingston.

David Last is the Secretary of the International Society of Military Sciences and teaches Political Science at the Royal Military College of Canada.

Odin Bartsch is a former editor of the Queen's University Journal Federalism-e and now serves as a Public Affairs officer in the Canadian Armed Forces.

The International Society of Military Sciences (www.isofms.org) is a consortium of defence universities in small democratic countries that collaborate for mutual improvement.

The Polish Association for Security aims to improve security in the broadest sense through education, prevention, and collaboration.

NATO's Defence Education Enhancement Program (DEEP) is a collaborative initiative that supports partner nations in reforming and strengthening their professional military education systems through curriculum development, faculty training, and strategic guidance.

Building Defence Capabilities for Future Uncertainty

Edited by
Laurenz Fürst, Ugurhan Berkok, David Last and Odin Bartsch

NATO DEEP eAcademy
International Society of Military Sciences, and
Swedish Defence University

2026

Cover image: developed by Copilot from composite images.

Building Defence Capabilities for Future Uncertainty

First published 2025 by NATO DEEP eAcademy Press
Uniwersytet Warmińsko-Mazurski w Olsztynie ul. Michała Oczapowskiego 2 10-719 Olsztyn, Poland

and the Polish Association for Security and War Studies University of Poland, (Akademia Sztuki Wojennej) al. gen. Antoniego Chruściela "Montera" 103 00-910 Warsaw-Rembertów, Poland.

This publication is part of the Defence Education Enhancement Programme (DEEP) series inspired by collaboration with the International Society of Military Sciences (www.isofms.org)

The content of this publication does not reflect the official opinion of the North Atlantic Treaty Organization or other official positions of organizations associated with its publication or its contributors. Responsibility for the information and views expressed in this book lies entirely with the authors and the editors.

ISBN: 978-83-975616-3-2

Reviewers:
Assoc. Prof. Piotr Gawliczek, PhD
COL Assoc. Prof. Andrzej SOBOŃ, PhD, Eng.

© 2025 selection and editorial matter, Laurenz Fürst, Ugurhan Berkok, David Last, Odin Bartsch. Individual chapters, the contributors.

The right of Laurenz Fürst, Ugurhan Berkok, David Last and Odin Bartsch to be identified as the authors of the editorial material, and of the authors for their individual chapters has been asserted in accordance with sections 77 and 78 of the Copyright, Designs and Patents Act 1988.

This work, Building Defence Capabilities for Future Uncertainty, edited by Laurenz Fürst, Ugurhan Berkok, David Last, and Odin Bartsch, is licenced under Creative Commons Attribution NonCommercial ShareAlike Licence 4.0 by NATO DEEP eAcademy Press and the War Studies University of Poland.

You are free to share, copy and redistribute the material in any medium or format. The licensor cannot revoke these freedoms as long as you follow the licence terms:

Attribution – You must give appropriate credit and provide a link to the licence.

Non-commercial – You may not use the material for commercial purposes.

No Derivatives – If you remix, transform, or build upon the material you may not distribute the modified material.

No additional restrictions – You may not apply legal terms or technological measures that restrict others from doing anything the licence permits.

Notices:

You do not have to comply with the licence for elements of the material in the public domain or where your use is permitted by an applicable exception or limitation.

No warranties are given. The license may not give you all of the permissions necessary for your intended use. For example, other rights such as publicity, privacy, or moral rights may limit how you use the material

Disclaimer: corporate logos and any other company or organization or branding represented are specifically excluded from the Creative Commons Attribution NonCommercial ShareAlike Licence 4.0 of this work and may not be reproduced without the express written permission of the copyright holders.

Permissions:

Figure 3.1. *Submarine Cable Map* TeleGeography, submarinecablemap.com, Creative Commons License: Attribution-ShareAlike 4.0 International (CC BY-SA 4.0).

Figure 4.1, *Hierarchical Tactical Communication Architecture for Platoon-Level Operations*, is reproduced from Suomalainen, J., Julku, J., Vehkaperä, M., & Posti, H. (2021), *Securing public safety communications on commercial and tactical 5G networks: A survey and future research directions*, *IEEE Open Journal of the Communications Society, 2*, 1590–1615, under the Creative Commons Attribution 4.0 International License (CC BY 4.0). © 2021 The Authors.

Figure 23.1. *World Military Expenditure by Region, 1988–2023*, is reproduced with permission from Tian et al. (2024), *Trends in world military expenditure, 2023*, Stockholm International Peace Research Institute. © SIPRI. All rights reserved.

Figure 24.1. *Typical SSCL Workplan.*
Source: Space Strategies Consulting Ltd., 2025. Used with permission. All rights reserved.

Table 9.1: *Differences between systems engineering and SoS "engineering"* reproduced with permission from: INCOSE. (2018). *Systems of Systems Primer*. International Council on Systems Engineering (INCOSE). © INCOSE. All rights reserved.

Figures ix

Tables xi

Contributors xii

Acknowledgement xxii

Foreword xxiii

List of Abbreviations xxv

Introduction: Conflict Today and the Uncertainty of Future Wars, David Last xxx

Section 1: Strengthening Domestic Defence xlix

Chapter 1: Integrating Human Rights and Emerging Technologies in Defence Capabilities: A Framework for Ethical Resilience, Marco Marsili 1

Chapter 2: Approaches to Assess Troop's Resilience in Defense, Oleksandr Maistrenko 19

Chapter 3: The legal challenges in the protection of submarine cable, Ahmed Abdel Hakam 37

Chapter 4: Robustness of Tactical and Military Networks Against Natural Disasters and Hostile Environments: A Comprehensive Analysis of Military Communication Systems Resilience, Abdellah Chehri and Dorota Domalewska 58

Chapter 5: The role and legal status of military intelligence in combatting hybrid threats, Eerik Heldna 90

Section 2: Modernization of Military Capabilities 109

Chapter 6: Forming an Analytic Framework for the Communication of the Military Utility of Technology, Kent Andersson and Patrik Stensson 110

Chapter 7: The impact of hybrid threats on operations in modern warfare. 130

Chapter 8: Do Drones Dream of Transparent Battlefields? Dealing with Past and Future Alternatives to the Tactical Crisis in Contemporary Warfare, Sandro Teixeira Moita 146

Chapter 9: Negotiation as a Key Enabler Behind Multi-Domain Operations, Pedro B. Àgua, Vitor Conceição, and Anacieto Correia 157

Chapter 10: A Contemporary Taxonomy of Information Warfare: An Analysis Proposal Based on Scientific Production, Mariana Grilli Belinotte and Luiz Rogério Franco Goldoni 172

Chapter 11: The Significance of News as an Aspect of Information Operation in the South China Sea Conflict, Bagus Jatmiko, Marseito, and Irhamni Ali 203

Chapter 12: Building EU defense capabilities for energy-tech hybrid warfare from Russia and China, Maurizio Geri 224

Chapter 13: Wargaming Tomorrow's Threats: Fostering Critical Thinking Through Simulation-Based Learning, Tali Neumann 237

Chapter 14: Geopolitical Futures and Force Structure Planning, Robert Addinall, Ali Dizboni, and Peter Gizewski 250

Chapter 15: Terrorism in Armed Conflicts: A Breach of Norms or an Element of Strategic Culture as per Example of the Russian Federation and Soviet Union, Maria Juczewska 262

Section 3: Improving Professional Military Education 280

Chapter 16: Shaping Our Future: Reflections and recommendations on professional military education at the Royal Military College of Canada, Isaac Nitschke..... 281

Chapter 17: Addressing the Digital Deficit in Professional Military Education, Christopher Morris and Veronika Hinman 297

Chapter 18: Critical thinking – what is it good for? Kyrre Tromm Lindvig..... 312

Chapter 19: Embracing Digital Transformation in Professional Military Education: Maintaining Relevance, Resilience, and Success, William Combes..... 323

Chapter 20: Before 'Skynet': Cultivating Digital Phronesis in Canadian Military Professional Development Programs, Anne Reiffenstein..... 352

Section 4: Fostering Public-Private Cooperation..... 363

Chapter 21: Military Capability Development in Europe: Considering a Normative Ecosystem Perspective, Johanna Jungwallius..... 364

Chapter 22: Enhancing European Ammunition Production: Strategic Responses and Challenges, Roland Hellberg and Martin Lundmark..... 379

Chapter 23: Beyond the Battlefield: The Military's Role in Climate Resilience, Khalid Mahmood Shafi and Jens Vesterlund Mathiesen..... 405

Chapter 24: Force Multipliers: Providing Quality Advice to Defence and Security Stakeholders, Harry Kowal and André Dupuis 424

Chapter 25: Unlocking Policy Performance with Organisational Innovation – Public-Private Partnerships' Potential for Grand Strategy Designs, Megghi Pengili..... 433

Figures

Figure 2.1: *An equations that reflects the interrelationship between the resilience and performance of two opposing sides* 30
Figure 2.2: *A system of Lotka-Volterra equations that reflects the mutual influence of two opposing sides* 31
Figure 2.3: *Dynamics of parameter changes with higher resilience of our unit (higher recovery rate and lower losses during combat interaction)* 32

Figure 4.1: *Hierarchical Tactical Communication Architecture for Platoon-Level Operation*s..... 60
Figure 4.2: *Impact and Risk Assessment of Natural Disasters and Environmental Hazards.*..... 61
Figure 4.3: *Illustration of the Integration between Stable Network Topologies and Mobile Tactical Networking through SATCOM Systems*. 65
Figure 4.4: *Tactical Mobility Management Strategies.* 65
Figure 4.5: *Mesh Network Features.* 67
Figure 4.6: *Space-Terrestrial Network Resilience*. 69
Figure 4.7: *Optimization of Wireless Communication and Frequency Management in Tactical Networks.* 73
Figure 4.8: *Securing tactical communication from easily detectable to undetectable*. 74
Figure 4.9: *Communication Systems in Perspective: Contrasting Technical Capabilities and Applications.* 77
Figure 4.10: *Evaluating Communication Systems: A Comparative Analysis of Technologies and Performance.* 78
Figure 4.11: *Enhancing power and energy resilience.* 81
Figure 4.12: *Enhancing urban research and Rescue Coordination*. 83
Figure 4.13: *Core Functional Elements of Integrated Emergency Operations Centers*. 85

Figure 6.1: *illustrates the concept of Fighting power, or in Swedish, Krigföringsförmåga* 114
Figure 6.2: *illustrates the Swedish Armed Forces' Traceability Model* 116
Figure 6.3: *illustrates the dynamics between capability components. The relational diagram, referred to here as the Development-eight* 118
Figure 6.4: *illustrates a model of capability development where the development-eight is placed in a context represented by scenarios and described across four decision horizons: here and now, soon, then, and later. In a Swedish context, typically five years are added for progressively longer decision horizons, corresponding to the political strategic defence review period.* 120

Figure 9.1: *Critical Success Factors and Necessary Conditions for Achieving the Goal* 162
Figure 9.2: *CRT - defining the problem links the UDEs to root causes* 165
Figure 9.3: *FRT – designing the solution through injections INJ 1-5* 166
Figure 9.4: *The prerequisites tree for injections INJ2 and INJ3* 169

Figure 10.1: *Article dispersion by year and number of citations, distributed in qualitatively determined periods.* 178
Figure 10.2: *Publication patterns as analysed using changepoint package.* 179
Figure 10.3: *Article dispersion by publication year and citations. Highlighted articles were selected for qualitative analysis*. 180
Figure 10.4: *Distribution of documents by type*. 184
Figure 10.5: *Annual production by document type (1990–2024)*. 185
Figure 10.6: *Annual growth rate of scientific production (1994–2024)*. 185
Figure 10.7: *Cumulative scientific production (1990–2023).* 187

Figure 10.8: *Average citation count by publication year.* 188
Figure 10.9: *Cumulative citations over time (1990–2024).* 188
Figure 10.10: *Relationship between output and citations: other document types* 189
Figure 10.11: *Relationship between output and citations: articles.* 190
Figure 10.12: *Top-cited documents based on citation count.* 191
Figure 10.13: *Top 20 most frequent authors by number of publications*. 192
Figure 10.14: *Top-cited authors based on total citations.* 192
Figure 10.15: *Top-cited authors based on average citations per article.* 193
Figure 10.16: *Technology Dependency by Period.* 194
Figure 10.17: *Destinatary by Period*. 195
Figure 10.18: *Relationship Tech x Destinatary* 196
Figure 10.19: *Target by Period.* 197
Figure 10.20: *Relationship Destinatary x Target*. 197
Figure 10.21: *Relationship Tech x Target.* 198
Figure 10.22: *Distribution of analyzed articles by target, destinatary, technological dependency, and publication period (1982-2024)*. 199

Figure 11.1: *The source counts of the mainstream media and news platforms*. 207
Figure 11.2: *Predicted Topic of News Articles* 209
Figure 11.3: *Cloud of keywords on the topic of information operation and warfare in the SCS based on the Countries mentioned*. 211
Figure 11.4: *Percentage of the Topic Findings* 212
Figure 11.5: *Sentiment Analysis Results on Tone* 213
Figure 11.6: *Sentiment Analysis on Subjectivity and Polarity* 213
Figure 11.7: *Time Series Analysis on the South China Sea Issues* 215

Figure 13.1: *A comparative table mapping key cognitive biases to specific Structured Analytic Techniques (SATs) that help counteract them, emphasizing the practical application of analytical tools.* 239
Figure 13.2: *A conceptual framework diagram illustrating how red teaming and SATs interact to foster critical thinking by encouraging adversarial analysis, structured exploration of alternatives, and systematic bias mitigation.* 242
Figure 13.3: *A timeline representing the sequential phases of Wikistrat's simulation-based learning process.* 242

Figure 14.1: *Impact Uncertainty Axes and Alternative Futures* 252
Figure 14.2: *Mapping the Four Worlds on the Continuum of Campaign Themes* 256

Figure 22.1: *Units of Analysis* 382

Figure 23.1: *World Military Expenditure by Region, 1988-2023* 409
Figure 23.2: *DIME Model of Climate Military Nexus* 419

Figure 24.1: *Typical SSCL Workplan* 427

Tables

Table 3.1: Comparing Aspects of UNCLOS Articles 48

Table 6.1: *Presents a preliminary proposal for a framework for analysing communication around technical forecasts within the context of capability development*. 126

Table 9.1: *Differences between systems engineering and SoS "engineering"* 161
Table 9.2: *The TOC has four fundamental questions* 163
Table 9.3: *The Categories of Legitimate Reservation* 164

Table 10.1: *PRISMA protocol steps* 175
Table 10.2: *Comparison of periodisations obtained through qualitative analysis and statistical changepoint detection.* 179
Table 10.3: *Coding scheme used to classify the articles by target, destinatary, and tech dependency.* 182

Table 11.1: *Topic Modelling* 210
Table 11.2: *Trigram Analysis Results* 216

Table 23.1:*Summary of Key Policy Recommendations* 416

Table 25.1: *Knowledge Development and Individual Learning Expertise* 447
Table 25. 2: *Knowledge Combination and Community Learning Effectiveness* 453
Table 25.3: *PPP's contribution to Grand Strategic Designs* 455

Contributors

Robert Addinall (Ph.D., RMC, MA, BA University of Toronto) is a sessional instructor in the Public Administration programme and History departments at the Royal Military College of Canada and an independent strategic analyst. His prior work includes studies on Canadian armoured vehicle procurement, the Future Security Environment (FSE) and the organizational history of the Canadian Army Land Warfare Centre (CALWC). His research interests include military history, history of technology, political science, and strategic foresight. Examples of his publications include: "The Long Engagement: The Case of the Canadian Army's Multi-Mission Effects Vehicles," in the *Canadian Army Journal* 14, no. 3, [2012]; Book Review of *12 Seconds of Silence: How a Team of Inventors, Tinkerers, and Spies Took Down a Nazi Superweapon* by Jamie Holmes in *Canadian Army Journal*, 20.2, 2024; and, in collaboration, Addinall, Robert; Gizewski, Peter, *The Future Security Environment: Design and Science and Technology (S&T) Implications for Army Functional Operating Concepts*. Scientific Letter, DRDC-RDDC-2018-L304, Defence Research and Development Canada, December 2018; and Addinall, Robert; Dizboni, Ali; Gizewski, Peter, "Observations from Canadian Army Futures Work and the [Un]Changing Character of War: Extremism and Maximalism 2016-2024" in *KCIS 2023: The [Un]Changing Character of War*, edited by Alison Brown and Howard G. Coombs. Queen's University Centre for International and Defence Policy, 2023.

Pedro B. Agua: Professor Pedro Agua teaches General Management, Project Management and Defence Systems Acquisition, as well as Negotiation at the Portuguese Naval Academy. He has been the Portuguese Navy Research Centre Deputy Director from 2023 to the end of 2024, and a national representative with the NATO STO for the Systems Concepts and Integration, particularly with a Focus on Systems-of Systems and Complex Adaptive Systems. A former Naval Officer, he combines his teaching profile with an extensive business background of more than 28 years as senior manager, dedicated to cutting edge fields such as defence, telecommunications and subsea industry, leading systems engineering and project management teams across several countries. A former graduate from the Portuguese Naval Academy specialized in Weapons and Electronics, he also holds an Executive MBA from AESE and IESE Business School and a Ph.D. in Industrial Engineering and Management awarded by the University of Lisbon.

Irhamni Ali is an experienced Data scientist and holds a PhD in Data Science from the University of North Texas, He dedicated his career to advancing knowledge and innovation in the field of data science. With this expertise, He has had the privilege of serving as a Lead Data Scientist at the National Library of Indonesia, where He has leveraged data-driven insights to drive informed decision-making and improve library services. Throughout his career, his research interests have been at the intersection of data science, machine learning, and advanced data analytics and he has published numerous papers on these topics. In the future, he expects to contribute to the ongoing conversation about the role of data science in multidisciplinary perspectives.

Lt-Col. Kent Andersson is currently senior lecturer and associate professor in Systems Science for Defence and Security at the Swedish Defence University while still an active officer in the Swedish Armed Forces. His research interests lie in systems for defence and security, with a particular focus on the development of military capabilities and methods for assessing the implications of technological advancements.

Mariana Grilli Belinotte is a PhD candidate in Military Sciences at Brazil's Army Command and Staff College (ECEME), having completed a visiting scholar period at King's College London (KCL). She holds a Master's degree in Law from the Federal University of Minas Gerais (UFMG) and a Bachelor's degree in Law from the University of São Paulo (USP). Her doctoral research explores cyber power and its implications for defense and sovereignty. She has published in peer-reviewed journals and has presented her work at international conferences, including the International Studies Association Annual Convention and the International Society of Military Sciences Conference. She is a columnist for Diário de Minas newspaper, contributing to policy discussions on contemporary security issues and is currently a visiting professor in geopolitics at Pontifical Catholic University of Minas Gerais (PUC Minas, Brazil).

Dr. Abdellah Chehri, P.Eng., SMIEEE (chehri@rmc.ca) is a Full Professor in the Department of Mathematics and Computer Science and Associate Vice Principal of Research at the Royal Military College of Canada (RMC) in Kingston, Ontario. He also holds affiliate and adjunct academic appointments at the Université du Québec en Outaouais (UQO), Université du Québec à Chicoutimi (UQAC), and the University of Ottawa. Dr. Chehri earned his Ph.D. in Electrical Engineering from Université Laval. His research interests span emerging technologies such as the Internet of Things (IoT), public safety communications, advanced wireless systems, and the integration of artificial intelligence and machine learning into next-generation networks. He has played a leading role in organizing and chairing several international conferences and symposia, including serving as Program Chair for the International Conference on Human-Centred Intelligent Systems and Tutorial Co-Chair for both the IEEE World Forum on Public Safety Technology (WF-PST) and the IEEE Canadian Conference on Electrical and Computer Engineering (CCECE). His involvement extends to key global events such as IEEE ICC, Globecom, WCNC, and FNWF, where he has chaired tracks, symposia, and workshops. Dr. Chehri is a licensed Professional Engineer in the province of Quebec and a Senior Member of IEEE. He actively contributes to the Communications Society, Vehicular Technology Society (VTS), and Photonics Society, advancing the global research community through editorial service, technical program leadership, and collaborative innovation.

Captain William "Bill" Combes, USN (retired), is Director of Leadership and Management Studies and Chair of the Digital Transformation and Artificial Intelligence Working Group at the Baltic Defence College, Tartu, Estonia. With 27 years of naval service including submarine command and Pentagon strategic planning roles, he leads strategic initiatives in military education focusing on innovation leadership and management, critical thinking development, and AI integration. An IPMA Level A certified portfolio director, his team delivers professional military education across multiple courses, supervises research, and manages international partnerships advancing project management excellence in multinational defence contexts. His current research examines human-AI collaboration in professional military education, systematic approaches to digital transformation in multinational institutions, and the development of transferable frameworks for responsible AI adoption in military contexts. You can contact me at william.combes@baltdefcol.org or https://www.linkedin.com/in/wmcombes/.

Vítor Plácido da Conceição is a Portuguese Navy Captain (Reserve) with over three decades of operational and academic experience in navigation, maritime safety, and defence education. A graduate of the Portuguese Naval Academy (1994), he served as Commanding Officer at sea and held leadership positions in the Hydrographic Institute, Naval Research Centre, and Naval Academy, where he was Academic Dean (2022–2025). He holds an MSc in Positioning and Navigation Technology (University of Nottingham) and is completing a PhD at Chalmers University of Technology, researching human factors, socio-technical systems, and resilience in maritime navigation. A lecturer and researcher since 2014, his work bridges operational expertise

and innovation in defence education, simulation, and human-technology teaming. Now in reserve status, he focuses on interdisciplinary research and advancing education and decision-support systems for complex, high-stakes environments.

Anacleto Correia is an Associate Professor at the Portuguese Naval Academy, where he lectures on Management and Information Systems. He holds a Ph.D. in Computer Science, an M.Sc. in Statistics and Information Management, a B.Sc. in Management, and a B.Sc. from the Portuguese Naval Academy. His research spans business and requirements engineering, software development methodologies, process modeling, data mining, and machine learning. With over 30 years of experience leading high-impact software development projects, he has consistently contributed to cutting-edge solutions across defense and enterprise domains. He is the author of several books and has published more than one hundred peer-reviewed papers in international journals and conference proceedings.

Ali (Al) G. Dizboni (Ph.D., MA, l'Université de Montréal) is an Associate Professor and the Chair of MSS (Military and Strategic Studies Programme) at the Department of Political Science and Economics at the Royal Military College of Canada. He is also an Associate Fellow with leading research centers such as CIDP (Queens' University). His current research include the Formation of Wahhabi State in Saudi Arabia, the genesis of Ballistic Missiles in Middle East (three case studies) and Right-Wing Radicalization in selected NATO Armed forces. Examples of his publications include: in collaboration, *A Hermeneutic Analysis of Military Operations in Afghanistan,* Palgrave-Macmillan; in collaboration *"Future Trends of Canadian Military Operations in Middle East",* , McGill & Queen's University Press; journal paper *"La République islamique et le fait minoritaire" Diplomatie*; book chapter in collaboration *"The Terrorist Resourcing Model applied to Canada"*, *Journal of Money Laundering* ; book chapter in collaboration, on Framing, Branding and Explaining: A Survey of Perception of Islam and Muslims in Canadian polls, Government, and Academia, Oxford University Press; Book chapter in collaboration on Instruments and Arrangements Against Online Terrorism Relating To International Cooperation, with Taylor & Francis Publisher. His latest publication in collaboration is with Parameters Journal on Developing Strategic Lieutenants in the Canadian Army (2022) He is an occasional commentator for the French, English/Persian media on different aspects of Middle East/Iranian politics and the Canadian Foreign policy in the region. Dr Dizboni is fluent in four languages English, French, Persian and Arabic.

Dorota Domalewska is an Associate Professor at the National Security Faculty, War Studies University, Poland, where she also serves as Director of the Doctoral School. Her interdisciplinary research lies at the intersection of security studies, communication, and education, with a particular focus on social cybersecurity and political and social threats in the digital information space. She has led and participated in several research projects funded by the Ministry of Science and Higher Education, the National Science Centre, and the Ministry of National Defence in Poland. Since 2016, she has been an Associate Editor and, since 2020, the Editor-in-Chief of Security and Defence Quarterly. She is also an Editor of Applied Cybersecurity and Internet Governance and a member of the Advisory Board of the Journal of Security Strategies (Güvenlik Stratejileri Dergisi). In 2012, she was a lecturer at Stamford International University in Thailand and, from 2012 to 2015, at Rangsit University, where she also held a research fellowship in 2019.

Colonel (Retired) Andre Dupuis has over 35 years of experience in the Canadian Armed Forces in Air Defence and Space operations, mission execution and strategic planning. Throughout his career, he has been selected to lead numerous highly visible command and transformational initiatives. He led the Canadian Space Cadre during his last 8 years in the service

and had a key role in the recognition of the importance of space operations to the Canadian Forces. His last Job in the Department of National Defence was as the Acting /Director General Space and the Director of Space Requirements, where he was responsible for all aspects of the delivery of space capabilities to the Forces. Upon his retirement he founded Space Strategies Consulting Limited, a company dedicated to providing trusted third-party advice to the commercial, civil, and national security space enterprise.

Dr Maurizio Geri is an EU Marie Curie Postdoc fellow with a 3-year project 2024/2027 between GMU in Washington and Ca' Foscari in Venice, to research the EU-NATO strategies against Russian/Chinese and other rivals' hybrid warfare, in the 'energy/resources/technology' security nexus. He is also an Italian Navy Lieutenant Commander reservist, working as a Foreign Policy Advisor for the MOD General Staff, in particular for the EU operation IRINI commanded by Italy. He holds a PhD in International Security from ODU in Virginia/US, an MA in Cultural Studies, and a BA in International Relations, from the University of Florence, Italy. He is a former analyst for various NATO bodies in the US (NATO ACT), Italy (CMRE/JFCNP), and Brussels (NATO HQ). He has experience with different think tanks in the US, including Carter Center, Washington Institute for Near East Policy, and Global Policy Institute, and in Italy (Center for the Innovation of Defense and Euro Gulf Information Center). In his youth, he also worked as a field officer in the Global South with different NGOs (including Peace Brigades International and Nonviolent Peace Force). Dr Geri has published a book (https://www.springerprofessional.de/ethnic-minorities-in-democratizing-muslim-countries/27389182), some academic articles (https://digitalcommons.usf.edu/jss/vol17/iss3/2/), and several op-eds/journalistic articles (https://muckrack.com/maurizio-geri/articles).

Peter J. Gizewski is an Adjunct Professor in the Department of Political Science and Economics, Royal Military College of Canada (RMCC), and Fellow at the Center for International and Defence Policy, Queens University. A recently retired Defence Scientist with Defence Research and Development Canada's Center for Operational Research and Analysis (DRDC-CORA), he served as Strategic Analyst to the Canadian Army Land Warfare Center (CALWC) for over 20 years and was a core contributor to the CALWC's Future Army Project - a multi-volume study exploring the capability requirements for Canada's Army -- circa 2040. He was educated at the University of Toronto (Trinity College) and Columbia University. His research interests include the future of deterrence, strategic foresight, United States foreign and defence policy and arms control and disarmament.

Professor Luiz Rogério Franco Goldoni studies cybersecurity, cyber defense, and strategic studies at Brazil's Army Command and Staff College (ECEME). He holds a PhD in Political Science with emphasis in Strategic Studies from the Federal Fluminense University (2011) and serves as coordinator of the Defense Management research line and the Cyber Power Laboratory (LPCiber) at ECEME's Graduate Program in Military Sciences. His research focuses on cyber power, cybersecurity, and cyber defense, with publications in peer-reviewed journals including the Brazilian Journal of International Politics and Journal of Strategic Security. Dr. Goldoni has supervised numerous master's and doctoral theses on cybersecurity topics and participates in international academic conferences, including recent presentations at the International Studies Association. He has contributed to policy discussions through publications in major Brazilian newspapers and has been involved in Brazil's national cybersecurity policy development.

Ahmed Abdel Hakam is a Solicitor-Advocate before the Higher Courts of England & Wales and a French Avocat. He is a partner at Volterra Fietta in London and currently sits on the Dispute Resolution Committee of the Law Society of England & Wales. He is also member of the international law commission of the New York City Bar Association. Ahmed regularly advises and

represents States and multinational companies from North America, Europe and Asia, in disputes relating to: the consequences of civil war on a State's rights and obligations towards foreign investors; legal issues arising from the existence of competing governments; transboundary pipeline transit and transportation regimes; disputes relating to the construction of civil nuclear projects; and related international law issues arising from State dislocation. The author thanks Haoyu Rao, an associate at Volterra Fietta, for his research assistance in preparing this chapter.

Eerik Heldna is high ranking police officer, a reserve officer and a lecturer of law at the Estonian Military Academy. He holds a Master of Law degree from the University of Tartu and is a graduate of the FBI National Academy. Eerik has over 25 years of experience in law enforcement and the security sector. He has also served as the Deputy Commander of the Military Intelligence Centre. Throughout his extensive public service career, he has contributed to drafting national defence-related legislation, including the intelligence chapter of the Estonian Defence Forces Organisation Act and the National Defence Act.

Roland Hellberg (PhD) is a Senior Lecturer in War Studies at the Swedish Defence University in Stockholm. He has over 25 years of research experience in the field of logistics and more than 20 years of leadership experience in logistics-related operations. Dr. Hellberg's current research focuses on defence logistics, with particular emphasis on security of supply, defence industry supply chains, the logistical implications of military expansion, the role of logistics in Host Nation Support, and the integration of dual-use innovations and civilian resistance. He has published extensively in these areas, contributing significantly to both academic scholarship and policy discussions on military logistics and national defence preparedness.

Veronika Hinman (born Poniscjakova) is Deputy Director and Senior Teaching Fellow at the Portsmouth Military Education Team (PMET), University of Portsmouth, UK. She holds a PhD in International Relations from the University of Nottingham, with a research focus on political violence and terrorism. For the past six years, she has delivered professional military education (PME) at two Royal Air Force bases: RAF Cranwell and RAF Halton, teaching officer cadets and non-commissioned officers, respectively. This experience has shaped her academic interest in PME as both a teaching practice and a research area. Her broader research interests include international security, irregular warfare, and conflict studies. Veronika is a Fellow of the Higher Education Academy and regularly appears on international broadcast media to comment on defence and security issues.

Dr. Harry Kowal is a retired Brigadier-General and Principal Emeritus of the Royal Military College of Canada (RMC). His 42 years of service includes 33 years as an Air Force Officer and 9 years as Principal RMC. He was appointed to command three times and served as Director General Military Careers. His Governor-in-Council appointment as Principal carried with it responsibilities as special advisor to the Minister of National Defence and Academic Advisory to the Commander of the Canadian Defence Academy. He also served as an Executive Head with the Council of Ontario Universities and Universities Canada and as President of the Canadian Aeronautics and Space Institute. He is currently working as a consultant. Dr Kowal holds a doctorate, three master's degrees and professional military education (Command and Staff Course and Executive Leadership Program (Canadian Forces College) and National Securities Program (Australian Centre for Defence and Strategic Studies)).

Bagus Jatmiko is an Indonesian Navy officer who holds a PhD in Information Sciences from Naval Postgraduate School in Monterey, California. With a strong blend of academic expertise and operational experience, he has served in various command and staff roles across multiple levels of the naval organization. His background gives him a strategic perspective on maritime

defense challenges, particularly in the Indo-Pacific dynamic s ecurity environment. He currently leads the Wargame Center in the Indonesian Naval Command and Staff College. His research and professional focus lie in defense and security issues, particularly information operations and warfare, underwater infrastructure protection, and the responsible-AI in the military domain. He is a firm advocate for integrating emerging technologies to enhance national defense capabilities and maritime security posture. Furthermore, he champions a holistic approach in forwarding the future of defense, which lies in harmonizing cutting-edge technology with empowered personnel and agile organizations.

Maria Juczewska is a seasoned international professional with over a decade of experience in research and study across Europe and the United States. She holds two M.A. degrees and is currently a Ph.D. candidate in the Security Sciences at the War Studies University, Warsaw. A graduate in International Affairs from The Institute of World Politics in Washington, D.C., Mrs Juczewska specializes in international relations, U.S. statecraft, and the security landscape of Central and Eastern Europe. Her research experience includes presentations at international conferences in New York, Buffalo, Stockholm, Cracow, and Jastarnia, as well as invited lectures at West Point Academy and Georgetown University. In 2018-2019 she doubled as a Research Fellow in Polish Studies of the Victims of Communism Memorial Foundation, where she focused on bringing Polish history to American audiences. As a perpetual learner, Mrs Juczewska brings a well-rounded and original perspective to her scholarly investigation in security sciences.

Lt-Col Johanna Jungwallius is a Military Teacher at the Swedish Defence University. She holds a master's degree in War Studies, with a focus on military strategy, security policy, and defence policy. At the Department of Systems Science for Defence and Security, she teaches theory and research methodology within the Joint Advanced Command and Staff Programme. She has previously served as Chief of Staff at the tactical level and as Chief of Plans at the Air Warfare Centre. Her contribution to this book draws on extensive experience in the Swedish Air Force, particularly in the fields of capability development and quality assurance. She is also engaged in academic research on norm dynamics in security policymaking, and her peer-reviewed research has been published in the Scandinavian Journal of Military Studies

David Last is a Commonwealth Scholar and Fulbright Fellow, who served for thirty years in the Canadian Army with tours in Cold War Germany, Cyprus, former Yugoslavia, and research and teaching in the Middle East, West Africa, and Asia. He has been teaching political science, public administration, and war studies at the Royal Military College of Canada since 2000, with secondments to the Canadian Forces College, Privy Council Office, and Non-Commissioned Member Leadership College. He has been Secretary to the International Society of Military Sciences since 2017.

Lieutenant-Colonel Kyrre Tromm Lindvig is an active-duty Norwegian Army officer. He has served in a variety of positions on a tactical and operational level and has extensive experience from international operations. Deployments include among others Afghanistan (both ISAF and RSM), Mali (UN) and the Middle East (OIR). He is currently teaching at the Staff College of the Norwegian Defence University College. He defended his Ph.D in cultural studies at the University of Oslo in 2008. In addition, he was visiting research student at the Hebrew University in Jerusalem 2011–2013 and he is an alumnus of the Senior SOF leadership course at the Nato Special Operations University in Belgium. His research interests include special forces operations, the role of humanities in military thinking and education, military and tactical intelligence as well as cultural studies.

Martin Lundmark (PhD) is a Senior Lecturer in the academic institution systems science for defence and security at the Swedish Defence University in Stockholm. He has over 25 years of research experience in the field of defence acquisition, defence industry, defence innovation and related topics. His PhD Transatlantic Defence Industry Integration (2011) was published in the field of business administration at the Stockholm School of Economics. Current research focuses on defence logistics with particular emphasis on security of supply, and defence industry supply chains; organization of military prototype development and dual-use innovation; multilateral arms collaboration. He joined the Swedish Defence University in 2017. Prior to that he worked at the Swedish Defence Research Agency (FOI) 1998-2017. He has been a guest researcher at MIT (Boston) and Fondation pour la Recherche Stratégique (FRS, Paris). He has published in these areas, contributing significantly to both academic scholarship and policy discussions on military logistics and questions related to defence industry and defence acquisition.

Col. Oleksandr Maistrenko is a Doctor of Military Science and a Professor of the Department of Special Operations Forces of the National Defence University of Ukraine. He is a Specialist in Rocket and Space Systems, Aviation and Cosmonautics Engineer. He holds a Master of Combat Application and Management of the Land Forces Units Actions and a Doctor of Military Sciences, PhD in Military Arts, Professor in the Armaments and Military Equipment sphere. His scientific interests are the evaluation of the effectiveness of the functioning of military systems, Resilience of the functioning of human-technical systems, Military education, Training of PhD students, Ballistics. He held various positions in the Armed Forces of Ukraine serving in several combat roles including senior operator, service chief, battery commander, division chief of staff, division commander; and several scientific roles such as doctoral student, leading researcher, head of the research department, associate professor, professor, deputy head of the department, and head of the department. He directly participated in the Russian-Ukrainian war in 2015, and 2022.

Marco Marsili is a researcher with a focus on international relations, international (humanitarian) law, human rights, and the implications of emerging technologies on global 18 security. He holds a PhD in History, Security Studies and Defense and has published extensively on topics related to cognitive warfare, cybersecurity, and the intersection of technology, international (humanitarian) law and human rights. He has directed international research projects, and collaborated with EDA, NATO STO, DIANA, and the Centre for Advanced Defence Studies (CASD)/Institute for Defence Research and Analysis (IRAD) of the Italian Ministry of Defence. Dr. Marsili is affiliated with Cà Foscari University of Venice, where he integrates the Research Institute for International Studies, and can be reached at info@marcomarsili.it/marco.marsili@unive.it. ORCID: 0000-0003-1848-9775. For further info: https://www.marcomarsili.it.

Jens Vesterlund Mathiesen is a Special Advisor and researcher at the Center for Stabilisation, at the Royal Danish Defence College's (RDDC) Institute for Strategy and War Studies. He is the Head of Programme for the RDDC Afghanistan-Pakistan programme financed by the Danish Peace and Stabilisation Fund, and has been researching security, defence and diplomacy in the region and beyond. His teaching and research focuses primarily on international stabilisation operations, Afghanistan after August 2021 and the role of climate change in military affairs. He is the co-editor of the SJMS Anthology: "Still Here: Understanding and Engaging with Afghanistan after August 2021" from 2024. He holds a master's degree in political science from Aarhus University.

Sandro Teixeira Moita holds a PhD in Military Sciences. He is a professor in the Postgraduate Programme in Military Sciences at the Brazilian Army Command and General Staff College. He teaches Strategy, Intelligence and Operational Art. He is the coordinator of Minerva,

the Conflict, Strategy and Intelligence Research Group. He acts as an advisor to several operations of the Brazilian Army and the Cabinet of Institutional Security of the Presidency of the Republic.

Christopher J. Morris is a Wargaming and Modelling Subject Matter Expert with Calian Europe, currently working at the NATO Joint Warfare Centre in Stavanger, Norway. He holds a PhD in Law and has a strong academic and operational background in counter-terrorism, violent extremism, and threat analysis. Prior to his current role, he served as a Teaching Fellow in Air and Space Power at the University of Portsmouth, delivering professional military education in partnership with the Royal Air Force. His experience also includes lecturing in policing and international relations, and field experience in the middle east. Christopher has led funded research projects, and regularly publishes on topics such as radicalisation, military pedagogy, and digital learning. He is a Fellow of the Higher Education Academy and an active member of the Military Operations Research Symposium and the Society for Terrorism Research.

Marsetio is a former Chief of the Indonesian Navy with the last rank of admiral. He is also a full professor at the Indonesian Defense University (IDU), Jakarta, Indonesia, with a research focus on the maritime security domain. He is currently positioned as the special advisor for the minister of science and high education of the Republic of Indonesia. He has extensive experience in both academic and practical aspects of maritime security. During his time as the Chief of the Navy, his focus is to build collaboration between the ASEAN navies in the framework of confidence-building measures (CBM). In his time now, he is a prolific writer and a keen researcher with writings in articles, journals, and books. His focus is mostly on maritime security in the South China Sea.

Acting Sub-Lieutenant Isaac Nitschke is a graduate of the Royal Military College of Canada with a bachelor's in military and strategic studies. Upon graduation, he commissioned as an officer in the Royal Canadian Navy and began graduate studies at Queen's University (Kingston, Ontario), pursuing a Master of Arts in Political Studies focusing on International Relations. His research interests focus on defence and security policy, in particular maritime security, information warfare, and hybrid warfare.

Tali Neumann is the Head of Marketing and Digital Platforms at the crowdsourced consultancy Wikistrat. She holds a B.A. in Psychology and Business Administration from Tel Aviv University (TAU). With nearly a decade of experience in media-related roles, she has worked in public relations and advertising, served as a military journalist in the Israeli Defense Forces (IDF), and later as a commander at the IDF Spokesperson's Military Journalists' course.

Megghi Pengili specialises in defence innovation governance, defence ecosystems and knowledge management, energy defence resources and cybersecurity in the Eastern Mediterranean, AI-Public Private Partnerships and Anticipatory Governance in defence, and other defence issues. She is a Visiting Fellow at the University of Leeds, where she obtained her PhD in Innovation's Governance and Defence Studies. She holds an MA in International Relations from the University of Sussex and an Executive Master in EU Studies from the Centre Internationale de Formation Européenne. Two- time "George C.Marshall Centre" Scholar (2007 & 2025) and Blavatnik Centre for Interdisciplinary Cyber Studies Visiting Fellow (2021-24), she has received many European and international scholarships. She worked in national and international defence establishments before academics. She has taken numerous military and defence courses in Italy, her native country, and abroad. She was Civil Wars Journal's Assistant Editor (2022-24). Megghi joined TRENDS US as Senior Advisor in March 2025.

Anne Reiffenstein, CD, is a retired artillery officer who served in the Canadian Army for 28 years, joining in 1989 as part of the early generation of women in the combat arms. Throughout

her career, she took on diverse roles in operations, strategic and tactical planning, defence resource management, professional military education, training development, and leadership. Following her military career, Anne has embraced new challenges, hosting and producing podcasts and multimedia projects, teaching in business schools and professional military education programs, and consulting on learning development, education, and military professional development. She is a Doctoral candidate in Business Administration at Royal Roads University, exploring digital phronesis—the intersection of digital ethics, decision-making, and leader development—with a focus on how to cultivate it in leaders.

Lt-Col. Patrik Stensson holds a MSc in engineering physics and a PhD in Informatics from Uppsala University. He is currently the Chief Scientist of the Swedish AirForce and is also a lecturer at the Swedish Defence University. His research interests lie in the (necessity of the) human role in making technology truly useful (and morally justified), in practice, and therefore in particular the difficult human position (regarding for example possibility of control and responsibility) in relation to AI-enhanced information systems and so-called autonomous systems.

Col. Viktor Savchenko (born 19 July 1980) is an officer in the Marine Corps of the Armed Forces of Ukraine. He holds a master's degree in strategic studies (USA, 2022) and in Combat Employment and Command of Ground Forces Units (National Defense University of Ukraine, 2015). He has extensive command and staff experience at operational and operational-strategic levels, including roles as Chief of Combat Training of an Airborne Brigade and Chief of Operations of the Marine Corps Command. He served in peacekeeping missions in Iraq (2004–2005) and Kosovo (2008–2009), and participated in NATO exercises in North Macedonia, Poland, Jordan, and Montenegro. He has collaborated with international working groups to coordinate foreign partner support. His professional expertise includes planning, evaluation, and implementation of transformation processes in the Armed Forces of Ukraine, as well as operational-level risk management. He is married and has three children.

Dr. Khalid Mahmood Shafi is an accomplished researcher, academician, and practitioner, with three decades of experience in climate change, disaster management, policy advocacy, conflict resilience, and security. He served in a senior leadership role, commanding operations in conflict zones for over three years, and also a year with UN. Academically, Dr. Shafi has been Professor of Practice at NUST and served as Director at ISSRA, leading strategic research initiatives. He earned a postdoctoral fellowship at Copenhagen Business School and holds a PhD, focused on climate–security nexus. He has authored two books on climate policy (one with a foreword by former UN Secretary General Ban Ki Moon), published extensively in peer reviewed journals, and serves as editor of a reputed journal. He has designed and taught postgraduate and professional courses on climate securitization and is a frequent speaker at academic forums. He can be reached at LinkedIn and khalidmayo@hotmail.com

Acknowledgement

The idea for an international collaboration between defence universities in small countries was born in discussions between Allard Wagemaker and Alexander Bon of the Netherlands Defence Academy (NLDA) and Walter Feichtinger of the Landesverteidigungsakademie (LVAK). The International Society of Military Sciences was launched in Amsterdam in May 2008 by representatives of the Austrian National Defence Academy, the Netherlands Defence Academy, the Baltic Defence College, the Norwegian Defence University College, the Swedish Defence University, the Royal Danish Defence College, the Finnish National Defence University, and the Royal Military College of Canada. The vision, energy, and continuing engagement of Walter Feichtinger (Austria), Hannu Kari (Finland), Alexander Bon (Netherlands), Niels Bo Poulson (Denmark), and the many other representatives and supporters from each institution have been essential to continuing the life of this organisation. The 18 annual conferences, rotating between institutional members, and the periodic workshop events for graduate students or on specific themes have made the ISMS a vibrant part of the international ecosystem for professional military education. It could not have evolved without the support of the Deans, Rectors and Commandants who make up the uneasy constellation of professional duty and academic freedom in each of our member institutions. At critical junctures, leaders have stepped up to rescue the ISMS when it threatened to cease working. Alexander Bon launched the Society's first website hosted in the Netherlands. Ryszard Szpyra brought Poland into the Society in 2016. Anders Sookermany (Norway) picked up the 2017 conference at short notice, and Ryszard Szpyra (Poland) hosted the tenth anniversary conference in 2018, inviting Commandants and Rectors to rejuvenate the Society and reaffirm its mandate. Harry Kowal (Canada) found funding for the Society's website, which is now funded by Canada until 2028. Hannu Kari (Finland) and David Last (Canada) mounted virtual conferences during the global Pandemic of 2020 and 2021. Anders Sookermany (Norway) has led the editing of the Handbook of Military Sciences, published by Springer and now available online free thanks to funding from the Norwegian Defence University College. Paulo Marreiros brought Portugal into the Society in 2023, and Andreas Rüdisüli has shepherded Switzerland's accession successfully. Kjell Engelbrekt (Sweden) negotiated the publication arrangement with NATO DEEP under which this volume and the preceding book of abstracts has been made available free online.

Everyone involved in this project has incurred many debts to insure its timely and effective completion. Unless otherwise noted, all views expressed are those of the authors, not necessarily any organisations with which they are affiliated.

Foreword

There are at least three reasons behind the abrupt shift, in the first half of the 2020s, from drowsy inattention to a reinvigorated focus on building new and better defense capabilities. One reason is the dizzying speed of technological evolution in the world's most advanced economies driven by rapid scientific innovation, intense competition and corporate profit-seeking, as well as war itself. Another is the growing political ambitions of several world leaders, apparently seeking to break free from the relative complacency of their post-Cold War predecessors. A third reason is the sheer necessity of scaling up defense forces and improving the skills of military professionals, in order to be in a position to deter and defend against adversaries not seldom influenced by the two aforesaid developments.

This volume speaks primarily to the latter set of issues. The powerful impetus experienced by governments and institutions charged with building new and better defense capabilities will no doubt serve to energize and accelerate the efforts of people, businesses and military organizations in the second half of the 2020s and beyond. The same goes for academies and universities responsible for the research and education of soldiers, officers and auxiliary civilian staff. It is not enough to simply ramp up production and activities, relying on legacy programs and generic knowledge. Before scaling up, military educational institutions must take into account how the world of warfare is changing in ways that substantively alter the preconditions for tactics, operations and strategy. Moreover, tomorrow's war will be fought with the capabilities that we design, acquire and deploy today (as well as with yesterday's equipment), along with doctrine developed to align with the former. In part, this presupposes careful reflection and planning rather than short-termism, so that defense capabilities are up to the tasks of the future. That being said, we also need to suppress the understandable desire to consistently optimize the new capabilities which we procure and instead make room for pragmatic adaptation and subsequent improvement once systems come online. Key qualities going forward must be defense capabilities that can be mass produced, are agile and deployable across a wide range of contingencies, and the software of which can be easily updated. For defense forces that rely on conscripts, ease of use must be factored in already at the design stage.

The 2024 ISMS Annual Conference placed a premium on scholarly and military-professional contributions that revolved around the overarching theme of competing priorities at a time of rising military expenditures: "Scaling Up, Learning Lessons, Ensuring Quality." In putting together this volume based on papers that in one way or another addressed this theme in the context of building defense capabilities, the authors and editors have sought to enhance our understanding of how to best weigh options that live up to all three of those fundamental objectives. In the transatlantic area and across the world, many of us will be preoccupied with getting the right blend of such priorities in the coming five to ten years.

Kjell Engelbrekt
President, International Society of Military Sciences (ISMS)
28 July 2025

Preface

In September 2024 soldiers and scholars from more than twenty countries gathered at the Swedish Defence University in Stockholm to present and discuss new research at the annual conference of the International Society of Military Sciences. The conference theme of *Scaling Up, Learning Lessons, Ensuring Quality* gave participants an opportunity to reflect on the rapid changes to global security since Russia's invasion of Ukraine in 2022. The Book of Abstracts has now been published as a record of every paper presented at the Conference. This volume serves to continue the discussion of a subject central to the military profession and national security. How can small countries build defence capabilities for an uncertain future?

Since September 2024, the world has become more uncertain, with continuing and evolving wars in Ukraine and the Middle East, and a new tariff war threatening to undermine the stability of the global economy while the US pushes its allies to spend more on defence. Parallel to the ISMS conferences in Stockholm (September 2024) and Amsterdam (October 2025) the NATO Defence Economics Working Group has met in Bordeaux and will produce papers by distinguished defence economists on how best to achieve and take advantage of the new and higher spending targets. As we focus on building capabilities in small countries, defence economics becomes everyone's business. These papers will be published separately.

The four sections of this collection address strengthening domestic defence, modernizing military capabilities, improving professional military education, and fostering public-private cooperation. Authors hail from the member and partner countries of ISMS, and we are pleased to welcome individual contributors from other countries, whether or not they are small and democratic. Contributions at the ISMS are welcomed from young scholars and new practitioners, and from grizzled veterans who bring decades of experience to the discussions. We are grateful to the many reviewers who have helped to advance the essential work of the Society, and our thoughts are with those who struggle for the security of their countries and the safety of their citizens in difficult times.

International Society of Military Sciences

Laurenz Fürst
Austrian Ministry of Defence
Chair of ISMS Working Group on Security and Defence Policy
Vienna

David Last
Royal Military College of Canada
2025 President Secretary
Kingston

Ugurhan Berkok
Royal Military College of Canada
Chair of the NATO Working Group on Defence Economics
Kingston.

Odin Bartsch
Royal Military College of Canada
Kingston

List of Abbreviations

ADF - Australian Defense Force
AI - Artificial Intelligence
ALE - Automatic Link Establishment
AMOS - Arctic Mobile Observation System
AOTD – Latvian Ministry of National Defence (*Antrasis operatyviniu tarnybu departamentas*)
APTs - Advanced Persistent Threats
ASAP - Act in Support of Ammunition Production
BLOS - Beyond-Line-of-Sight transmission
BLS - Bureau of Labor Statistics
BMOQ - Basic Military Officer Qualification
C2 - Command and Control
C2IS - Command and Control Information Systems
CAF - Canadian Armed Forces
CBP - Capability Based Planning
CCoR - Cadet Chain of Responsibility
CDS - Cross-Domain Solutions
CIMIC - Civil-Military Cooperation
CO_2 - Carbon Dioxide
CPSA - Canadian Political Science Association
CRMs - Critical Raw Materials
CRT - Current Reality Tree
CSF - Critical Success Factors
DAS - Distributed Acoustic Sensing
DE - Desirable Effects
DEIC - Defense Environmental International Cooperation
DIANA - Defence Innovation Accelerator for the North Atlantic
DIB - Defence Industrial Base
DIL - Disconnected, Intermittent, and Limited Networks.
DIME+E - Diplomacy, Information, Military, Economy, + Environment
DOD - US Department of Defense's
DRC - Disaster Response Communications
DSA - Dynamic Spectrum Access
DSSS - Direct Sequence Spread Spectrum
DTAIWG - Digital Transformation and Artificial Intelligence Working Group
DTIB - Defence Industrial and Technological Bases
EDA - European Defence Agency
EDF - European Defence Fund
EDI - Equity, Diversity and Inclusion
EDIP - European Defence Industry Program
EDIRPA - European Defence Industry Reinforcement through common Procurement Act

EDIS - European Defense Industrial Strategy
EDRT - European Defence Research & Technology
EDT - Emerging and Disruptive Technologies
EDTIB - European Defence, Technological and Industrial Base
EDTs - Emerging Disruptive Technologies
EEZ - Exclusive Economic Zone
EFIS - Estonian Foreign Intelligence Service
EMIC - The Estonian Military Intelligence Centre
EMP - Electromagnetic Pulse
EU - European Union
EW - Electronic Warfare
FCAS - Future Combat Air System
FHSS - Frequency Hopping Spread Spectrum
FRT - Future Reality Tree
FSO - Free-space optical
GDPR - General Data Protection Regulation
GenAI - Generative AI
GEO - Geostationary Satellites
GMACCC - Global Military Advisory Council on Climate Change
GRU - Russian military intelligence
HF - High-Frequency
HIPS - Host-Based Intrusion Prevention Systems
HUMIT - Human Intelligence
IAI - Israel Aerospace Industries
IBTS - Individual Battle Task Standards
IDF - Israel Defense Forces
IEEE 802.1AE - MACsec
IFTS - International Flight Training School
IHL - International Humanitarian Law
IHRL - International Human Rights Law
IJVs - Joint Institutional Ventures
INS - Intermediate Nodes
IoBT - Internet of Battlefield Things
IoMT - Internet of Military Things
IPR - intellectual property rights
ISE - Initial Support Estimate
ISR - Intelligence, Surveillance, and Reconnaissance
ISS - Estonian Internal Security Service
ITS - Intelligent Tutoring Systems
JAS - Security Authorities Act (julgeolekuasutuste seadus)
JIT - Just-in-Time

JRC - European Commission Joint Research Centre's
KAP - Knowledge, Attitude, and Practice
KAPO - Estonian Security Police (*Kaitsepolitseiamet*).
KKS - Defence Forces Organisation Act (kaitseväe korralduse seadus)
KM - Knowledge Management
LAWS - Lethal Autonomous Weapon Systems
LEO - Low Earth Orbit Satellites
LGS - Leonardo Global Solutions
MDO - Multi-Domain Operations
MEO - Medium-Earth Orbit Satellites
MFA - Multi-Factor Authentication
MIC - Military-Industrial Complex
MIDD - Latvian Defence Intelligence and Security Service, (*Militārās izlūkošanas un drošības dienests, saīsināti*)
MIPv6 - Integration of Mobile IPv6
MNs - Mobile Nodes
MoD - Ministry of Defence's
MP - Military Police
NATO - North Atlantic Treaty Organization
NC - Necessary Conditions
NCOs - Non-Commissioned Officers
NEMO - Network Mobility Protocols
NKVD - People's Commissariat for Internal Affairs
NOAA - US National Oceanic and Atmospheric Administration
Nordefco - Nordic Defence Cooperation
NPM - New Public Management
NVIS - Near Vertical Incidence Skywave
OI - Organisational Innovation
OSINT - Open-Source Intelligence
PD - Professional Development
PER - Performance Evaluation and Review
PFS - Perfect Forward Secrecy
PL - Project Leader
PLARF - The People's Liberation Army Rocket Force
PMCs - Private Military Companies
PME - Professional Military Education
PMIPv6 - Enhancements to Proxy Mobile IPv6
PMO - Program Management Office
PPPs - Public Private Partnerships
PPT - Physical Performance Test
QKD - Quantum Key Distribution

R&T - Research and Technology
RF - Radio Frequency
Riigikogu - Parliament of Estonia
ROC - Resistance Operating Concept
ROTP - Regular Officer Training Plan
S&T - Science and Technology
SAB - Constitution Protection Bureau (*Satversmes aizsardzības birojs*)
SAFE - Security Action for Europe
SATCOM - Satellite Communication
SCS - South China Sea
SDN - Software-Defined Networking
SDP - Software-Defined Perimeters
SDRs - Software-Defined Radios
SECI - Socialization-Externalization-Combination-Internalization
SFIA - Skills Framework for the Information Age
SHF - Super High Frequency
SIGNIT - Signals Intelligence
SIPRI - Stockholm International Peace Research Institute
SMEs - Small and Medium Enterprises
SOEs - State-Owned Enterprises
SoI - System of Interest
SoS - Systems-of-Systems
SSCL - Space Strategies Consulting Ltd
TACSAT - Tactical satellite communications
TCNs - Tactical Communication Networks
TCP/IP - Transmission Control Protocol/Internet Protocol
TOC - Theory of Constraints
TSR - Time, Space, and Relative Strength
UAE - United Arab Emirates
UAVs - Unmanned Aerial Vehicles
UDE - Undesirable Effects
UHF - Ultra-High Frequency
UK - United Kingdom
UN - United Nations'
UNCLOS - United Nations Convention on the Law of the Sea
UNDP - United Nations Development Programme
UNEP - United Nations Environment Programme
UNESCO - United Nations Educational, Scientific and Cultural Organisation
UPS - Uninterruptible Power Supplies
USAFNC - US Air University Negotiation Centre
VC - Axon Ventures Capital

VDD - Latvian State Security Service *(Valsts drošības dienests)*
VHF - Very High Frequency Radios
VSD - Latvian civilian intelligence service *(Valstybės saugumo departamentas)*
WHO - World Health Organization
WPNP - US West Point Negotiation Project
ZT - Zero Trust
ZTA - Zero Trust Architecture

Introduction: Conflict Today and the Uncertainty of Future Wars

David **Last**, https://orcid.org/0000-0003-0447-4214

Defence institutions today face a convergence of pressures. Technology is evolving rapidly. Society is affected by new stressors. The world is geopolitically unstable. This is true around the world, but particularly urgent along Russia's long border, in the Middle East, and in Asia. With US moves on Greenland and foreign interference in Canada's debate about Alberta secession, North America is not immune. Meanwhile, in South Asia, Southern Africa and South America, rising powers are seeing new opportunities. NATO Europe and Canada have more than doubled their annual defence expenditures since Russia's seizure of Crimea in 2014. There is no simple solution for the range of grey zone and hybrid threats below the threshold of overt violence. The contributions to this book suggest a holistic approach, integrating domestic preparedness, modernized force development, professional education, and innovative partnerships. Future uncertainty ensures that military defence capabilities alone will be inadequate. Small democratic states feel a renewed urgency in calls for cooperation.

Growing Uncertainty and New Risks

We should begin by recapping how we got here. The bipolar structure of the Cold War gave way first in 1990 to unipolar American power. That dominance saw the emergence of multi-domain challenges to the West during the US-led Global War on Terror after Al Qaeda attacks of the 1990s, culminating in 9-11, 2001. Many Western states continued to enjoy a peace dividend of lower defence expenditures with sporadic contributions to cosmopolitan UN peacekeeping and stabilisation, while the US spent trillions of dollars on the wars in Afghanistan and Iraq. This period was interpreted very differently in the capitals and boardrooms of the West, and in the world against which the West is now rearming. While Western states relied on unparalleled US military supremacy, states unhappy with the Western order developed new tools for attacking it or defending themselves against it. Today, there is uncertainty at home, and growing threats from abroad, exacerbating the schisms within the West. Russia's leader is a former spy with delusions of imperial grandeur. Iran's oppressive theocratic regime has an asymmetrical global reach and behaves more like a religious movement than a state. China is a one-party state with expansive ambitions. The US, long a bulwark of the liberal international order, has turned transactional and threatens its allies.

We can look back for clues to future uncertainties. As the Cold War ended, US scholars like Robert Reich, Philip Bobbit, and David Rothkopf—all alumni of President Bill Clinton's cabinet and security council—tried to make sense of the new order. The end of Bretton Woods fixed exchange rates had preceded and perhaps accelerated the fall of Communism. The new mobility of capital, China's accession to the World Trade Organisation, deregulated markets, and multinational corporations were thought to spell an evolution beyond the nation states that had dominated the international order since the 1648 Treaty of Westphalia. Reich prescribed a new focus on empowering citizens to compete in a global economy (1992). Taking a long historical view, Bobbitt (2002) concluded that the nation state was being succeeded by forms of market state; China, Europe, and the US represented three different varieties of market state, in which state management, state regulation, and market mechanisms prevailed respectively. Rothkopf (2012) saw the emergence of super-citizens like the tech billionaires, and semi-states without the capacity for full sovereignty. All three authors converged on the idea of competing forms of capitalism with varying attempts to harness or constrain the power of corporations in a global economy. Economic historian Branko Milanovic (2019) confirmed that capitalism alone had survived what Bobbitt described as the long war of the twentieth century. Milanovic reinterpreted the history of communism as an alternative path to industrial and subsequently post-industrial capitalism.

More alarming for us today is Milanovic's criticism of the liberal interpretation of history:

> "The existence of World War I creates an insurmountable obstacle to the Whiggish interpretation of history: it just should not have happened. The fact that it happened at the heyday of liberal dominance, both nationally and in international relations, opens up the possibility that the liberal order might lead to a similar outcome in the future. And it is clearly impossible to claim that a system that might regularly end up in worldwide wars somehow represents the pinnacle of human existence, as defined by the quest for prosperity and freedom…1989 brings the world back to the path it was on in 1914." (Milanovic 2019:71-72)

The shock of the 2008 financial crash accelerated resistance to neoliberal globalization amongst Western electorates (Gerstle 2022) and enthusiasm for unregulated markets amongst elites (Mirowski 2011). Populist nationalism resembling early twentieth-century fascism is again on the rise in the Western states most enthusiastic about markets. Karl Polanyi described this pattern looking back at the origins of the Second World War (Polanyi 1944). When markets crush people, they look to states or strong leaders for salvation.

After the end of the Cold War, authoritarian regimes felt besieged, and liberal regimes felt vindicated. The Soviet Union shattered and successor regimes faced colour revolutions demanding democracy (Beacháin & Polese 2010). China faced a student revolt put down in Tiananmen Square in 1989 (Francis 1989). Authoritarian regimes from Morocco to Syria faced the social-media-fuelled Arab Spring (Ozekin & Akkas 2014). Whatever the truth about the sources of these pressures, authoritarian leaders interpreted them as evidence of a Western assault. Most Western citizens did not see themselves or their states at war, but significant anti-Western decision-makers did, in Russia, Iran, and China. If we are honest, we must add the United States to this axis of decision-makers pursuing war openly and covertly in ways that make future peace less likely and the outcomes of war more uncertain.

For Western democracies, Russia is at the heart of future threats despite having a shrinking population less than half that of the US, and a GDP less than half that of Germany. At the Munich Security Conference in February of 2007, Vladimir Putin accused the West of hostility: “NATO has put its frontline forces on our borders… It is obvious that NATO expansion represents a serious provocation that reduces the level of mutual trust.” (Stavrou 2025:19). In April 2007 sustained distributed denial-of-service (DDoS) cyber-attacks were experienced by the Estonian government, banks, and media after Tallinn moved a Soviet war memorial. Russia launched a hybrid war against Georgia in 2008, seizing parts of South Ossetia and Abkhazia in an attack that included conventional forces, cyber-attacks, information operations, and territorial revisionism, designating the population of the occupied areas as Russians (Tugushi 2024). 2009 to 2013 were characterized by cyber probing of Latvia, Lithuania, and Estonia, expansion of Russian overseas media RT and Sputnik, and investment in online influence networks. In November 2013 Moscow pressured Ukraine to abandon its EU Association Agreement using economic coercion, information operations and political interference. Crimea was annexed in an unflagged covert military operation in February-March 2014, followed by escalating proxy warfare in the Donbas region. In April 2015 there was a serious cyber-attack on the German Bundestag. From June to November 2016, according to the Mueller Report, Russia engaged in hacking, leaks and social-media manipulation to influence the outcome of the US election (Mueller 2019:50-59). The UK Parliament’s Digital, Culture, Media and Sport Committee concluded that Russian efforts aimed to increase tensions and undermine Britain’s democratic process during the Referendum to leave the EU (Danzig 2025). In 2018 Russian agents attacked defector Sergei Skripal in the UK with a nerve agent. 2019 saw large-scale cyber-disruption and political destabilization in Georgia between the presidential and parliamentary elections. From June to December 2021, Russia pushed migrants through Belarus as a coercive tool to destabilise the border regions of Poland, Lithuania, and Latvia.

February 2022 saw a full-scale conventional invasion of Ukraine. Russia responded to Finnish and Swedish accession to NATO with an orchestrated influx of migrants along Finland's borders in 2023, while the illegal migrant pressure on Poland fluctuates up to the present day (Koinova 2025).

Iran has regional aspirations with global ramifications. Ayatollah Ali Khamenei advocated forward defence (*defa'-e pishdast*) in a speech to IRGC commanders in 2013: "the language and message of this Revolution could not naturally be confined to the borders of Iran." (Khamanei 2013). Qassem Soleimani's command of the Islamic Revolutionary Guard Corps (IRGC) in 1998 became an inflection point for Iranian external operations using the Shi'a community and increasingly the disaffected Islamic diaspora in Western countries (Azizi 2020). Building Hezbollah in Lebanon (1992-1997) was the proof of concept for a proxy deterrent using asymmetric warfare. With US invasions of Afghanistan and Iraq, Teheran perceived encirclement, and Iraq became the central front from 2003 to 2010. With the Arab Spring of 2011-2014, the IRGC organized *Liwa Fatemiyoun* (Afghan fighters), *Liwa Zainabiyoun* (Pakistani fighters) and Iraqi militias, all deployed to Syria in the first multinational IRGC coalition. Khamenei's *defa'e pishdast* became the strategic justification for IRGC extraterritorial operations. The Islamic State in the Levant (ISIL, ISIS, or Da'esh) was a Sunni organization seen as inimical to Iranian interests, and the IRGC coordinated closely with Russia and Hezbollah supporting the Syrian regime in Damascus in 2015-2017. Despite Qassem Soleimani's assassination by the US in 2020, the IRGC consolidated and diversified, achieving wider reach with exports of drone technology to Hezbollah, the Houthis, Hamas, and Russia. In 2021 they expanded cyber operations targeting Israel, the Gulf states, the US and European states. Europe and Canada increasingly became theatres for money-laundering, influence operations, and espionage (Lorimer 2025). Iranian Russian cooperation has expanded since Russia's attack on Ukraine (Waller et al 2025). Iranian operations in Europe include attacks on Israeli and Jewish targets through the Foxtrot Gang (Iran International 2025), and active recruiting of gang members for missions to sabotage infrastructure in Sweden, Denmark, and Germany (Deconinck 2025).

Rush Doshi has described the evolution of China's expansive foreign and security policy, pushing back against US hegemony, with inflection points in 2008 ("actively accomplish something") and 2016 ("great changes unseen in a century"). Unlike the tide of kinetic and disruptive attacks from Russia and Iran, China's influence in the global community has been more ambiguous. China has generally supported sovereignty and has been consistent in condemning foreign interference in internal affairs. The Cyber defence company FireEye reported 13 active China-based groups conducting network compromises against corporations in the US, Europe and

Japan in 2015-2016. Regional spear-phishing campaigns targeted European organisations, reflecting Chinese security concerns (FireEye 2016). Canadian Security Intelligence Services (CSIS) annual report in 2017 warned of PRC influence targeting diaspora communities and political candidates. In 2018, European agencies attributed intrusions to Chinese state-linked actors targeting telecoms and research (AIVD 2019). In 2019, warnings came from Czechia and Norway that the PRC was targeting 5G infrastructure and research institutions. In 2020, investigations in the UK, Belgium, Spain, and Canada revealed PRC-linked “service centres” or “police service centres” monitoring Chinese nationals abroad, and serving as hubs for interference, intimidation, and harassment (Hardie 2023:1-2). In 2021, The Canadian Security Intelligence Service (CSIS) warned of PRC efforts to influence candidate nominations and diaspora voting in Canada. UK and German authorities identified targeting of ministries, parliaments and political parties by the PRC hacking group APT31 (Pomfret and Tian 2024). In 2023, Canada’s Communication Security Establishment (CSEC) warned of PRC targeting critical infrastructure and universities. Europol announced arrests and investigations into PRC-linked attempts to acquire intellectual property for semiconductor and advanced materials (Europol 2024). In 2025, Joint intelligence advisories warned of PRC groups targeting telecoms, transport, lodging, and military networks in more than 80 countries (CISA 2025).

The behaviour of the US under President Trump has exacerbated the sense of risk and uncertainty in the West. Trump has repeatedly questioned the value of NATO and suggested that Washington might not come to its allies’ defence, encouraging strategic opportunism by Russia. Trump has fractured the unified Western response to Russian aggression, reduced security assistance programs, threatened intelligence sharing, and disrupted long-standing multilateral planning. Tomas Jarmalavicius, Head of Studies at the International Centre for Defence and Security in Tallin, Estonia, said in March 2025 that it is increasingly difficult to keep the US engaged in Baltic defence while Baltic states are supporting Ukraine (Allik 2025). The US continues to pressure Greenland (Gettleman et al 2026) and exacerbate threats of Alberta Separatism in Canada (Kolga et al 2026).

Building defence capability for the future uncertainty of war must proceed in parallel with managing the current uncertainty of wars now in progress in the grey zone below the threshold of armed conflict, and the protracted wars on Russia’s borders and in the Middle East. Researchers affiliated with the International Society of Military Sciences (ISMS) and the European Research Group on Armed Forces and Society (ERGOMAS) have produced two volumes on grey zone conflict: *Modern War and Grey Zones: Design for Small Countries* (Routledge, 2026), and the free

e-book, *Policing the Grey Zone* (NATO DEEP, 2005). This volume continues that work by focusing on building defence capabilities for the eventuality of war which the ongoing grey zone conflicts seem to presage. Defence capabilities go well beyond purely military capabilities, which must be integrated within a national strategy. Preparing for a clash of forces in geographically defined battlefields is not enough; capabilities must address complex, hybrid, multidomain challenges. Capability development cannot be siloed. The four sections of this book begin to map the architecture for building future capabilities in these times of uncertainty.

Section 1: Strengthening Domestic Defence

Credible defence postures begin at home, with institutions that are legally grounded, resilient, adaptive, and capable of protecting the critical systems that underpin national life. Domestic defence cannot be limited to territorial security. For liberal democracies, it must encompass the preservation of human rights and civil society, the legal protection of critical infrastructure, and robust national communication and intelligence systems. This demands consideration of emerging technologies, including their potentially corrosive effects. The psychological and social resilience of troops, their families, and communities are a core capability, not a background factor. Submarine cables, space assets, critical infrastructure, and intellectual property all add legal vulnerabilities through foreign ownership, control and influence, and through contracted sabotage and manipulation. Communications networks serve as the backbone of operations at home or abroad. Integrated intelligence supports both immediate response and longer-term planning.

In Chapter 1, Marco Marsili presents a framework for addressing emerging defence capabilities in ways that promote ethical resilience for small democratic countries. Artificial intelligence can be used in conjunction with cyber intrusions to project risks of subversion or fifth-column attacks within a state. AI guidance, facial recognition, and cheap ubiquitous drone technology already make targeted personal attacks possible (Scott-Geddes 2024). The Russian war on Ukraine has accelerated troubling combinations of technology. Marsili advocates a collaborative approach involving government, international organizations and civil society to develop guidelines and best practices that sustain capabilities suitable to urgent defence needs, but compatible with democratic societies.

How do we know when troops are resilient? In Chapter 2, Colonel Dr Oleksandr Maistrenko clarifies “defence resilience” from the standpoint of an experienced military practitioner, cutting through the conceptual drift that surrounds the term across technical, humanitarian, and doctrinal

communities. He frames resilience through the core components of combat power—doctrinal adaptability, troop readiness and technology, and the moral-psychological strength of personnel—showing how these interdependent factors shape real operational capacity. The chapter also underscores the difficulty of translating resilience into quantitative indicators, arguing that meaningful assessment must account for correlation effects and the lived realities of force preparation and adaptation.

Attacks on critical infrastructure are part of the ongoing war in the grey zone below overt hostilities. In Chapter 3, Ahmed Abdel Hakam argues that submarine fibre-optic cables—carrying roughly 97 percent of global data traffic—have become indispensable to modern communication, commerce, and even military capability, yet remain highly vulnerable to natural hazards and deliberate interference. It shows that existing international legal frameworks, from the 1884 Telegraph Convention to UNCLOS, provide only partial and outdated protection, leaving significant gaps in enforcement and coordination. The conclusion underscores how contemporary threats—from seismic events to disruptions by State and non-State actors such as the Houthi militias—expose the inadequacy of current regimes and the persistent disconnect between cable operators and coastal States. Hakam calls for a more adaptive, robust, and cooperative legal architecture capable of safeguarding this critical infrastructure amid rising geopolitical and technological pressures.

Chapter 4 is a Canadian Polish collaboration on the resilience of military communications systems. Abdellah Chehri and Dorota Domalewska examine how military communication networks stay functional during natural disasters and hostile disruptions. The authors illustrate how architecture choices, redundancy, encryption, and rapid-deployment systems all contribute to resilience. Examples from combat zones and disaster responses illustrate how flexible routing, distributed designs, and cross-domain solutions help forces maintain command, control, and coordination under pressure. The Internet of Military Things in network-centric operations and cybersecurity is driven by emerging technologies—from AI-driven automation to quantum-secure encryption. It is reshaping next-generation military networks. Richly illustrated, the chapter offers a practical, forward-looking roadmap for strengthening resilient communications across contested and disaster-stricken environments.

In Chapter 5, Eerik Heldna, a senior police officer, reservist, and legal scholar examines how Estonia, working with neighbouring countries, has expanded the role of military intelligence in response to rising hybrid threats, while still operating within the constitutional principles that separate military and civilian authority. Using the Estonian case, the chapter shows how

democratic states must balance legal oversight with the practical need for intelligence services to gather information for national defence. Further to Chapter 3's argument that better legal regimes strengthen the protection of submarine cables, this chapter reinforces the point that liberal democracies—unlike their adversaries—treat law not as a constraint but as a source of legitimacy, clarity, and resilience. That commitment to legality becomes a strategic advantage: it creates clear mandates, strengthens public trust, and ensures that expanded security powers remain both effective and accountable.

Strengthening domestic defence goes well beyond military capabilities. Political, economic, social, technological, legal, and environmental factors are foundational. These chapters provide a starting point for integrating the factors that enable national security in the new environment.

Section 2: Modernizing Military Capabilities

Modernization is not just about acquiring better tools. New tools arrive at dizzying speed. Modernization demands reshaping military understanding of usefulness. How can emerging tools, like new social practices, AI, robotics, nanotechnology, energy, chemistry, and communications be used to generate or counter hybrid threats? Modernization should be seen as a system of systems, including conceptual approaches, new technology, information and its management, and organizational innovation. A theme uniting the ten chapters in this section is that human and intellectual capital are fundamental to modernizing military capabilities in multidomain operations. Future security challenges demand better analytical tools, stronger institutional cooperation, and more adaptive, evidence-based capability development. Together, these chapters argue that defence institutions must modernize intellectually as much as materially, building the cognitive, organisational, and technological agility needed to operate in an era of accelerating uncertainty and strategic competition.

Chapter 6 is useful for anyone looking for money from defence agencies to develop technology. How do you make the pitch? If you are spending money on defence technology, how do you decide if the expense is likely to be worthwhile? Two experienced military scholar practitioners, Kent Andersson and Patrik Stensson, provide an analytic framework to present the military utility of technology. Sweden is developing a clearer, more effective way to communicate about the military utility of emerging technologies at a time when rapid technological change and a worsening European security environment demand better forecasting. The authors identify seven conceptual starting points that shape dialogue between those who produce technical forecasts and those who rely on them for capability development, turning these into a set of guiding questions

that form an analytic framework. This framework is designed to help the Swedish Armed Forces make better use of expanding R&D investments by improving the way future capability concepts are discussed, assessed, and aligned with strategic needs. The chapter positions this as an evolving tool—one that will be refined through further empirical study to support more coherent, evidence-based capability development.

We are fortunate to draw on the experience of Colonel Viktor Savchenko, a serving senior officer in Ukraine's ongoing war. Chapter 7 analyses how Russia's war against Ukraine illustrates the growing impact of hybrid threats on modern military operations. Political, legal, informational, and kinetic tools—ranging from covert troop deployments and proxy forces to propaganda, cyberattacks, and sabotage—shaped the operational environment long before open conflict began. The chapter highlights why these methods are so difficult for commanders to detect and counter, and why democratic states are especially vulnerable to manipulation, legal ambiguity, and information attacks. It concludes that hybrid warfare is a strategy used by powerful actors. International cooperation, stronger legislation, corruption-resistant institutions, and better-prepared armed forces are essential for resilience in future conflicts.

Chapter 8, by Sandro Teixeira Moita of the Brazilian Army Command and General Staff College, offers a lively look at how drones—especially cheap, fast, soldier-operated systems—are reshaping the modern battlefield and creating what some call a "transparent" combat environment. Drawing on lessons from Ukraine and Gaza, Teixeira shows how constant aerial observation has changed infantry behaviour, troop psychology, and the balance between offense and defence. He argues that the way out of today's tactical stalemate is smarter integration: combining drones with armour, artillery, and infantry in a new manoeuvre-and-assault system. The chapter reminds readers that understanding how drones work in tactical, operational, and strategic contexts is essential if militaries want this new transparency to be an advantage rather than a costly surprise.

In Chapter 9, researchers from the Portuguese Naval Academy argue that effective Multi-Domain Operations (MDO) depend not only on advanced technologies and complex Systems-of-Systems, but on the human ability to negotiate across organisations with different priorities, cultures, and lifecycles. Drawing on systems-thinking methods, Pedro Água, Vitor Conceição, and Anacieto Correia show how decision-tree–based analytical tools—such as Categories of Legitimate Reservation, Current Reality Trees, and Future Reality Trees—provide the structured reasoning needed to diagnose friction points, align stakeholders, and build trust inside these sprawling systems. Negotiation, grounded in such decision-logic frameworks, becomes a core organisational capability without which MDO will fail to deliver its promised

"emergent effects." The chapter concludes that negotiation training should move from the margins of military education to its centre, especially as military–civilian integration becomes one of the most fragile links in achieving a truly effective MDO paradigm.

Chapter 10, written by two scholars from the Brazilian War College, maps the debate about "information warfare" over four decades. Drawing on nearly two thousand publications, Mariana Grilli Belinotte and Luiz Rogério Franco Goldoni show how the field has evolved from early, technology-focused concepts to contemporary understandings centred on narrative conflict, symbolic manipulation, and societal influence. Their proposed taxonomy—built around target (information or systems), recipient (society or military), and technological dependency—helps clarify how scholars use the term and why interpretations vary so widely. By tracing these shifts and highlighting global asymmetries in knowledge production, the chapter offers a structured way to analyse modern information campaigns without forcing a single definition onto a diverse and still-maturing field. This kind of understanding is foundational to modernizing capabilities to address new forms of warfare.

Chapter 11 continues in the vein of information, from the perspective of Indonesian naval officers engaged in Pacific operations. Bagus Jatmiko, Marsetio, and Irhamni Ali, experienced scholar-practitioners, examine how news media function as a strategic information operations tool in the South China Sea conflict. Using sentiment analysis, topic modelling, and data-driven methods, the authors show how China, the United States, and their partners use mainstream and alternative media to shape narratives, influence public opinion, and legitimize their positions. The chapter demonstrates how disinformation, misinformation, and selective framing become instruments of competition, revealing a broader "battle of narratives" that parallels military and diplomatic manoeuvring. It concludes by underscoring the need for critical media literacy and further research, as information operations increasingly shape both regional security dynamics and global perceptions of the conflict.

We move from information to hybrid warfare against European energy and technology, with Chapter 12. EU researcher Maurizio Geri outlines how the European Union must strengthen its defence capabilities to counter hybrid warfare from Russia in the energy domain and from China in the resources and technology sectors. The chapter explains that while initiatives like Re-Arm Europe mark an important start, the EU still lacks the common capabilities, strategic enablers, and integrated defence structures needed to deter and respond effectively. It argues that Europe must build a coherent strategy—clear ends, ways, and means—supported by joint procurement, resilient energy and technology infrastructures, deeper cooperation with NATO, and major reforms to the

European defence industrial base. In short, the chapter warns that hybrid threats are accelerating faster than Europe's ability to respond, making collective capability-building an urgent priority.

Chapters 13, 14, and 15 continue the theme of new forms of warfare demanding military modernization: critical thinking, force structure planning, and treating the breach of norms as an element of adversary strategic culture.

In Chapter 13, Tali Neumann of Wikistrat shows how red teaming and Structured Analytic Techniques, grounded in Wikistrat's simulation-based learning environment, offer a practical way to strengthen critical thinking in complex security contexts. By challenging cognitive biases, forcing assumption-testing, and enabling systematic evaluation of alternatives, these tools help prepare decision-makers for information-dense and manipulation-prone environments. The chapter argues that combining adversarial perspective-taking with structured analytic rigor provides an essential pedagogical framework for cultivating the analytical agility required for future defence challenges.

Chapter 14 examines how strategic foresight can illuminate emerging force-structure demands in an increasingly unstable international system. Revisiting the Canadian Army's earlier alternative-futures work, Robert Addinall, Ali Dizboni, and Peter Gizewski argue that today's environment resembles a "High-Tech Quagmire," where polarization, AI-driven information dynamics, and geopolitical assertiveness—not resource scarcity—drive insecurity. In such a world, states face pressure to field larger, technologically sophisticated, and more expensive full-spectrum forces, with small and medium powers confronting rising expectations for higher defence spending. The chapter underscores that in a polycrisis environment marked by unpredictability credible capability development becomes an existential requirement rather than a policy choice.

In Chapter 15, Maria Juczewska, a researcher at Poland's War Studies University, brings deep regional and historical expertise to her study of Russian strategic behaviour. She situates Russia's conduct in Ukraine within a longer continuum of Soviet and post-Soviet practices, arguing that the Russian Federation's systematic use of terror and terrorism is not an aberration but an entrenched feature of its strategic culture. Drawing on three conceptual approaches to terror and terrorism, as well as the notion of Russia as a counterintelligence state, the chapter shows how both covert sabotage and overt brutality against civilians "meet the criteria of terrorist activities" and reflect "historical and institutional continuity with the USSR. The chapter underscores how Russia's preference for force, intimidation, and revolutionary traditions produces a dual mode of warfare: a conventional campaign paired with systematic terror against civilian populations.

Juczewska highlights the paradox of a state that seeks global influence while relying on methods that undermine the very norms it claims to defend. Her analysis reinforces a central message of the volume: future defence planning must account for adversaries who deliberately disregard international law and employ terror as an integrated instrument of state policy, reshaping the global security environment in ways that demand new conceptual and operational responses.

Section 3: Improving Professional Military Education

Professional military education (PME) tunes the intellectual engine that drives enhanced defence capabilities. New defence capabilities demand adaptive thinkers who can navigate and thrive in complexity; executing doctrine is not enough. The five chapters in this section are focused on professional military education, no less important than the new technologies overshadowing military practice. In a period of apparent peace, have some educational institutions forgotten their primary purpose? Digital competence is essential but digital transformation of PME brings risks if it is not accompanied by critical thinking and the preservation of professional judgement.

Chapter 16, written by recent RMC graduate Isaac Nitschke, offers an insider's reflection on how Canada's professional military education system has been repeatedly reshaped by external reviews—most of them driven by domestic social, political, and cultural concerns rather than by operational requirements. The chapter argues that decades of scrutiny, from the Somalia Affair to the Arbour Report, have focused overwhelmingly on institutional culture, misconduct, and governance, often sidelining questions about how well RMC prepares officers for the emerging realities of conflict, including competition and coercion below the threshold of armed violence. Against this backdrop, the author contends that PME must be rebalanced: still attentive to ethics and culture, but far more tightly aligned with the operational, cognitive, and strategic demands facing junior officers in an era of grey-zone threats and renewed great-power rivalry.

Chapter 17 is by two authors from the digital education ecosystem linked to the UK Defence Academy. Christopher Morris and Veronika Hinman argue that modern militaries face a widening "digital deficit" at the very moment when contemporary weaponry—from networked sensors and autonomous platforms to cyber-enabled precision systems—makes digital competence indispensable for operational effectiveness. Drawing on UK examples, the authors show how traditional PME still anchored in historical case studies and bureaucratic routines struggles to prepare personnel for an era in which digital networks, data processing, and cyber defence shape everything from command decisions to the survivability of advanced weapons. They call for PME to become an experimental space for digital innovation, integrating hands-on simulation,

interdisciplinary training, and civil-military partnerships to build a force capable of operating, adapting, and defending the increasingly digital assets that now underpin national defence. Without a digitally literate force, even the most sophisticated modern weapons and defence systems cannot deliver their intended advantage. Digital competence has become as fundamental to military readiness as physical fitness or tactical skill. But consider this call in light of Reiffenstein's warnings of moral de-skilling and loss of judgement in a digitally enhanced environment (Chapter 20).

In Chapter 18, Norwegian staff college instructor and cultural studies researcher Tromm Lindvig argues that critical thinking is an essential but underdeveloped competency in professional military education. Rapid technological change and an increasingly contested information environment make critical thinking indispensable, but it is often crowded out by doctrinal conformity and process-driven teaching. This produces officers who "operate the machine" rather than question assumptions or adapt to new realities. Lindvig shows how this deficit hampers innovation, planning, and operational effectiveness, especially as adversaries exploit the cognitive and information domains through disinformation and influence campaigns—threats that require personnel (and citizens) able to discern narratives, evaluate evidence, and challenge faulty reasoning. Because critical thinking can be taught, he advocates introducing it early in PME and practising it continuously. Analysis of popular culture—from Hollywood films to non-Western war movies—is a low-cost, accessible way to train officers to interrogate identity, narrative, and representation. By doing this, PME can better prepare military professionals to navigate complexity, resist manipulation, and adapt to the accelerating pace of modern conflict.

In Chapter 19, William Combes of the Baltic Defence College argues that professional military education must undergo its own digital transformation if it is to prepare officers for NATO's rapidly evolving technological environment, where emerging and disruptive technologies—especially AI—are reshaping warfare, decision-making, and organisational culture. PME institutions face the dual challenge of modernising their own educational practices while approaching NATO's broader transformation agenda. Drawing on NATO policy, civilian educational innovation, and the Baltic Defence College's internal reforms, Combes shows that continuous experimentation, ethical AI integration, faculty development, and the systematic sharing of best practices are essential to maintaining relevance and resilience. The chapter concludes with examples of directives and activities for introducing artificial intelligence and digital transformation. These will be useful for other institutions.

In Chapter 20, Anne Reiffenstein, a former senior instructor at the Canadian Forces College, evaluates the consequences of digital transformation and artificial intelligence. In the Terminator movies, Skynet is a fictional US military artificial intelligence designed to manage strategic defence, but humans lose control. Reiffenstein argues we risk a more subtle and dangerous erosion of human judgement through "moral deskilling" as overreliance on machines diminishes leaders' judgement. She prescribes digital phronesis—practical wisdom for the digital age. Her chapter shows how digitization is reshaping warfighting and altering the human role in decision-making. Canadian professional development programs, in contrast, focus narrowly on digital literacy and overlook the deeper leadership and ethical demands of the digital era. Her three-part construct of digital phronesis aims to preserve human agency and responsibility through digital acumen, digital leadership, and digital ethics.

Section 4: Fostering Public-Private Cooperation

As defence challenges spill across governmental, commercial, and societal boundaries, the ability to mobilize public private ecosystems becomes a decisive strategic advantage for small liberal democratic states engaged in whole-of-society defence against larger neighbours. Developing new capabilities increasingly depends on networks of actors working in concert — industry, academic, civil society, and government.

In Chapter 21, Johanna Jungwallius of the Swedish Defence University argues that Europe's military capability development remains hampered by fragmentation, divergent national priorities, and inconsistent understanding of "capability development". Despite rising defence budgets and imminent threats from Russia, if not the US also, European states still struggle to coordinate planning, align defence industrial strategies, or exploit opportunities for synergy. These problems are intensified by legacy industries, path dependencies, and differing local conditions. Drawing on her research on defence industrial policy, the triple helix model, and cross-sectoral co-creation, Jungwallius proposes viewing capability development as an interconnected normative ecosystem rather than a set of isolated national or industrial activities. The chapter illuminates interdependencies between government, industry, and academia. Acknowledging the risks of oversimplification, Jungwallius argues that the ecosystem perspective encourages more integrated, adaptive and collaborative approaches, essential for the future of European defence production.

In Chapter 22, Swedish Defence University scientists Martin Lundmark and Roland Hellberg show how Russia's war against Ukraine has exposed a critical vulnerability in Europe's

defence posture: its ammunition production system, optimised for peacetime efficiency, cannot meet wartime demand. Ukraine's consumption rates have tripled European requirements, overwhelming supply chains already constrained by shortages of raw materials, explosives, skilled labour, and specialised machinery. Lundmark and Hellberg examine how EU initiatives—most notably the Act in Support of Ammunition Production (ASAP)—seek to rebuild capacity through targeted subsidies, long-term contracts, and coordinated investment. This creates difficulties in countries like Sweden, where procurement is market-driven and the state lacks ownership leverage. Drawing on interviews with industry and government officials, the authors argue that Europe must shift from transactional procurement to trust-based, strategic partnerships, rebuild domestic production of critical components, and strengthen dynamic capabilities across the supply chain. They contend that enhancing ammunition production is not merely an industrial challenge but a prerequisite for European strategic autonomy and credible defence in an era of sustained geopolitical instability.

Future uncertainty goes beyond the battlefield to encompass the rapidly evolving and increasingly unavoidable climate crises all states face. In Chapter 23, Khalid Mahmood Shafi of Pakistan's Institute for Strategic Studies and Research teams up with Jens Vesterlund Mathiesen of the Centre for Stabilization at the Royal Danish Defence College to address the military role in climate resilience. They argue that climate change has become a core security challenge, reshaping military operations, readiness, and strategic planning. Militaries occupy a dual role: they are major global emitters—largely exempt from climate reporting—and increasingly the first responders to climate-driven disasters. Drawing on securitization theory, human security, and cross-national case studies, the chapter shows how climate impacts degrade equipment, infrastructure, and logistics while simultaneously expanding military responsibilities in disaster relief. To reconcile these pressures, the authors propose embedding climate literacy into professional military education through the Knowledge–Attitude–Practice (KAP) framework and adopting a DIME+E approach that integrates environmental stewardship into national power. Their central claim is clear: climate-aware defence planning is no longer optional but essential to military effectiveness and national security in a rapidly warming world.

The public private ecosystem is an important advantage for small democratic countries. Chapter 24 is provided by a former Principal of the Royal Military College of Canada now working in the private sector. Harry Kowal and André Dupuis examine how the Canadian Armed Forces' post-pandemic recruitment and retention crisis has created a profound experience gap at precisely the moment when defence institutions face accelerating strategic, technological, and geopolitical

pressures. To bridge this shortfall, they highlight the growing importance of external expertise—civilian consultants acting as "force multipliers". They use Space Strategies Consulting Ltd. (SSCL) as a case study in civilian partners can help governments navigate complexity, maintain continuity, and generate advice when internal capacity is strained. This chapter complements Jungwallius's argument (Chapter 21) that capability development in Europe requires more integrate, ecosystem-based collaboration across government, industry, and universities. It also echoes Pengili's analysis of public-private partnerships (Chapter 25).

In Chapter 25, Megghi Pengili argues that in an era defined by hybrid threats, rapid technological disruption, and intensifying geopolitical crises, public–private partnerships (PPPs) have become essential engines of defence transformation and grand-strategy design. Drawing on Italian and Israeli case studies in cyber and aerospace, the chapter shows how PPPs function not merely as procurement mechanisms but as knowledge ecosystems that fuse government, industry, and expert communities. Through organisational learning, knowledge management, and innovation, PPPs help defence institutions anticipate future security environments, cultivate new operational concepts, and build resilience. Pengili demonstrates that PPPs act as "epistemic infrastructures," shaping strategic thinking by generating specialised expertise, enabling anticipatory governance, and aligning national defence goals with technological and industrial capabilities. In doing so, the chapter reframes grand strategy as a dynamic, knowledge-driven process—one increasingly co-produced by states and their industrial partners.

Toward an Integrated Architecture for Building Defence Capabilities

Taken together, the chapters in this volume argue for a defence posture built not on isolated strengths, but on integrated resilience: ethical, technological, educational, and collaborative. As small states build new capabilities, they must watch their backs. Ownership structures can be a vulnerability. Organized crime groups, gangs, and lone actors can be recruited online to target individuals, sabotage infrastructure, and disrupt supply chains. If we are to highlight a single change since these papers were prepared in 2024, it might be the changing role of the US under a second Trump administration.

Building defence capability is no longer just about acquiring equipment. The chapters in this book suggest that it is about building adaptive ecosystems of states, industries, knowledge communities, and partners in the whole of society. Only cohesive and adaptive ecosystems can respond to the accelerating strategic, technological and environmental pressures that small democratic countries face. History is unkind to those who confront rising danger in isolation. If we

cannot find the cohesion to prepare together, we may discover too late that we must endure the costs alone.

References

AIVD (2019) Annual Report 2018. General Intelligence and Security Service, Ministry of the Interior and Kingdom Relations. https://english.aivd.nl

Allik, H-L.(2025) Trump Positioning leaves Baltics walking a tightrope. Deutsch Welle, 9 March. https://www.dw.com/en/trump-positioning-leaves-baltics-walking-a-tightrope/a-71869374

Azizi, A.(2020) The Shadow Commander: Soleimani, the US, and Iran's Global Ambitions. One World.

Beacháin, D. and Polese, A., eds (2010) The Colour Revolutions in the Former Soviet Republics: Successes and Failures. Routledge

Bobbitt, P.(2002) The Shield of Achilles: War, Peace, and the Course of History. Anchor books.

CISA (2025) Cybersecurty Advisory: Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System. Cybersecurity and Infrastructure Security Agency, National Coordinator for Critical Infrastructure and Security Resilience. Revised 3 September. https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-239a

Danzig, J. (2025) How Brexit Played into Putin's Hands. EU ROPE, Ideas on Europe. 15 February https://eu-rope.ideasoneurope.eu/2025/02/15/how-brexit-played-into-putins-hands/

Deconinck, C. (2025) Migrant drugs gang in Sweden 'act as Iranian operatives' Brussels Signal, 27 June. https://brusselssignal.eu/2025/06/migrant-drugs-gang-in-sweden-act-as-iranian-operatives/

Doshi, R. (2021) The Long Game: China's Grand Strategy to Displace American Order. Oxford University Press.

Europol (2024) Uncovering the ecosystem of intellectual property crime: A focus on enablers and impact. Joint EUIPO-Europol strategic analysis report produced under EMPACT.

Fagan, M., Gubbala S. and Poushter, J. (2024) Views of Russia and Putin, Pew Research Centre, 2 July.

FireEye (2016) Redline Drawn: China Recalculates its Use of Cyber Espionage. FireEye iSight Intelligence. Special Report, June. https://services.google.com/fh/files/misc/rpt-redline-drawn-china-espionage-en.pdf

Francis, C. B. (1989). The progress of protest in China: the spring of 1989. Asian Survey, 29(9), 898-915. https://online.ucpress.edu/as/article-abstract/29/9/898/22606/The-Progress-of-Protest-in-China-The-Spring-of?redirectedFrom=fulltext

Gerstle, G.(2022) The Rise and Fall of the Neoliberal Order: America and the World in the Free Market Era. Oxford University Press.

Gettleman, J., Tekeli M., Troianoski, A. and Schmitt, E. (2026) In Closed-Door Talks, U.S. Demands a Major Role in Greenland, New York Times, 18 May. https://www.nytimes.com/2026/05/18/world/europe/us-greenland-talks-trump.html

Hardie, K. (2023) The Chinese Communist Party's Overseas Police Service Stations. Interim Report of the Special Committee on the Canada–People's Republic of China Relationship. Canada, House of Commons, 44th Parliament, 1st Session (November). https://www.ourcommons.ca/Content/Committee/441/CACN/Reports/RP12720365/cacnrp04/cacnrp04-e.pdf

Iran International (2025) US sanctions Swedish gang for alleged aid to Iranian attacks abroad, Iran International 12 March https://www.iranintl.com/en/202503129291

Khamanei, A.(2013) Leader's Speech in Meeting with Commanders of Islamic Revolutionary Guards Corps, 17 September. https://english.khamenei.ir/news/1827/Leader-s-Speech-in-Meeting-with-Commanders-of-Islamic-Revolutionary

Koinova, M. (2025). Power and informality in the polycentric governing of transit and irregular migration on EU's eastern border with Belarus. Journal of Ethnic and Migration Studies, 51(2), 501-525. https://www.tandfonline.com/doi/pdf/10.1080/1369183X.2024.2371214

Kolga, M., Phillips, J., McQuinn, B., Van de Walle, B., (2026) Decision Making and National Unity Under Threat: Foreign Interference, Cognitive Sovereignty, and the Alberta Referendum. CASI Labs, Canadian Digital Media Research Network, CipherAI, DisinfoWatch, and Global Centre for Democratic Resilience. https://disinfowatch.org/wp-content/uploads/2026/05/Alberta-and-Foreign-Interference-Report-Final-052026-web.pdf

Lorimer, S. (2025) Statecraft or criminality? Iran's covert operations and proxy networks in Europe. GSI-S https://gsi.s-rminform.com/articles/statecraft-or-criminality-irans-covert-operations-and-proxy-networks-in-europe

Milanovic, B. (2019) Capitalism, Alone: The Future of the System That Rules the World. Belknap Press, Harvard University.

Mirowski, P.(2013) Never Let a Serious Crisis Go to Waste: How Neoliberalism Survived the Financial Meltdown. Verso

Mueller, R.S. III (2019) Report on the Investigation Into Russian Interference in the 2016 Presidential Election. Volume I of II, Submitted Pursuant to 28 C.F.R. 600.8(c) Washington DC, March. https://www.justice.gov/archives/sco/file/1373816/dl?inline=

Ozekin, M. K., & Akkas, H. H. (2014). An empirical look to the Arab Spring: causes and consequences. *Alternatives: Turkish Journal of International Relations*, *13*(1&2), 75-87. https://ciaotest.cc.columbia.edu/journals/tjir/v13i1/f_0033740_27513.pdf

Polanyi, K.(1944) The Great Transformation: The Political and Economic Origins of our Time. Boston: Beacon Press.

Pomfret, J. and Tian, Y.L.(2024) APT31: the Chinese hacking group behind global cyberespionage campaign. Reuters. 26 March. https://www.reuters.com/technology/cybersecurity/apt31-chinese-hacking-group-behind-global-cyberespionage-campaign-2024-03-26/

PST (2019) Threat Assessment 2019. Norwegian Police Security Service (PST). https://www.pst.no/wp-content/uploads/2026/01/National-Threat-Assessment-2019.pdf

Reich, R.B.(1992) The Work of Nations: Preparing Ourselves for 21st Century Capitalism. Vintage Books.

Rothkopf, D. (2012) Power, Inc. The Epic Rivalry Between Big Business and Government—and the Reckoning That Lies Ahead. Viking.

Scott-Geddes, A. (2024) I Trained a drone to assassinate my boss. Telegraph/YouTube (21 November) https://www.youtube.com/watch?v=JeFMQuJ7qnk&t=149s

Souza, G. João P. (2025) The Weaponization of Migration: A Powerful Instrument in the Hybrid Warfare Toolbox [em linha]. APL Blog, Março 2025, NOVA Asylum Policy Lab, Faculdade de Ciências Sociais e Humanas, Universidade NOVA de Lisboa, DOI: https://doi.org/10.34619/qxp0-xq4k

Stavrou, O.(2025) Russia's War Against Ukraine: What Is It All About? Springer.

Tugushi, L.(2024) The 2008 Russo-Georgian War: Global Reactions and Long-Term Implications (November 06) SSRN: https://ssrn.com/abstract=5063257 or http://dx.doi.org/10.2139/ssrn.5063257

Waller, J.G., Wishnick, E., Sparling, M., and Connell, M. (2025) The Evolving Russia-Iran Relationship: Political, Military, and Economic Dimensions of an Improving Partnership. CNA (January). https://www.cna.org/analyses/2025/01/the-evolving-russia-iran-relationship

Yu Hua (2011) China in Ten Words. Pantheon.

Section 1: Strengthening Domestic Defence

Chapter 1: Integrating Human Rights and Emerging Technologies in Defence Capabilities: A Framework for Ethical Resilience

Dr. Marco **Marsili**, ORCID: https://orcid.org/0000-0003-1848-9775

Abstract:
As the global security landscape becomes increasingly complex and unpredictable, the need for robust defence capabilities that are both effective and ethically sound is paramount. This paper explores the intersection of human rights, emerging technologies, and defence capabilities, arguing that future military strategies must integrate ethical considerations to ensure resilience in an uncertain future. The rapid advancement of technologies such as artificial intelligence, cyber capabilities, and autonomous systems presents both opportunities and challenges for national security. While these technologies can enhance operational effectiveness, they also raise significant ethical concerns regarding privacy, accountability, and the potential for misuse. Among these, lethal autonomous weapon systems represent a particularly contentious area, as they challenge established norms of human control and responsibility in armed conflict. This paper proposes a framework for building defence capabilities that prioritize human rights and ethical standards, aiming to mitigate the risk that technological advancements may erode fundamental freedoms. The discussion will focus on three key areas: what capabilities should be built, who will build them, and how they will be built. It will advocate for a collaborative approach involving governments, international organisations, and civil society to develop guidelines and best practices that align defence strategies with human rights principles. By fostering a culture of ethical resilience, this paper aims to contribute to the discourse on sustainable defence capabilities that not only address immediate security needs but also uphold the values of democracy and human dignity in an increasingly volatile world.

Keywords: Human Rights Integration, Ethical Resilience, Accountability Frameworks, Ethical Standards, Military Ethics

Introduction

Technological innovations are redefining the global security landscape, creating unprecedented opportunities alongside significant risks. Emerging technologies such as artificial intelligence [AI], autonomous systems, and cyber capabilities are transforming the nature of conflict and military operations. However, this transformation does not come without consequences for human rights, raising pressing questions about the adequacy of existing

international frameworks in addressing these challenges. In this context, fostering ethical resilience becomes paramount to ensuring that technological innovation aligns with fundamental rights and democratic values.

Defence capabilities cannot be assessed solely in terms of efficiency or technological advancement; they must also be evaluated against their compatibility with fundamental principles of human dignity and justice. As highlighted in earlier studies (Marsili, 2022), contemporary military strategies often operate in ambiguous environments below the threshold of conventional armed conflict, underscoring the need for a robust and adaptable normative framework. This concern is well-established in the literature on civil wars and human rights, where scholars such as DeRouen and Heo (2007), Kalyvas (2006), and Weinstein (2007) have examined how irregular and fragmented conflict environments challenge the applicability of international legal norms and complicate efforts to protect civilians and uphold human rights.

Building on prior work examining dual-use innovation and decentralized AI governance (Marsili, 2025a; 2025b), this paper proposes a normative and operational framework aimed at aligning emerging military technologies with ethical and human rights standards. This contribution argues that integrating human rights into defence strategies is not merely a moral imperative but a practical necessity for ensuring long-term stability and security. In response to the inadequacies of existing normative frameworks, the concept of 'ethical resilience' is proposed as a strategic and conceptual tool to reconcile technological innovation with the preservation of universal values. By engaging in key theoretical perspectives and drawing on relevant case studies, the paper outlines a normative and operational framework for the development of ethical defence capabilities capable of addressing the complexities of contemporary and future conflict environments.

While emerging technologies encompass a broad and diverse array of innovations, this contribution does not aim to examine each category in detail. Instead, it focuses primarily on lethal autonomous weapon systems [LAWS], which present particularly acute ethical and legal challenges within the broader technological landscape.[1]

Key Concepts

In examining the intersection of military ethics, lethal autonomous weapon systems, and human rights, it is essential to first define key terms that will underpin the discussion: defence capabilities, human rights, and ethical resilience. Defence capabilities refer to the technological, strategic, and operational capacities that military forces develop to ensure national security. These

[1] For a detailed definition of emerging technologies, a discussion on how they differ from disruptive technologies, and a comprehensive list, see Marsili (2023a, pp. 25, 26, 32).

capabilities are increasingly influenced by the rapid development of advanced technologies, particularly those incorporating artificial intelligence and automation. Human rights, in the context of warfare, are principles designed to protect individuals from state violence, ensuring that military operations do not infringe upon the fundamental rights and dignity of persons, particularly civilians (Ruggie, 2011). Ethical resilience is the ability of a military force or defense system to adapt and respond to new technologies in a manner that aligns with ethical and human rights standards, even as the nature of conflict evolves (Marsili, 2025a).

The advent of LAWS raises significant ethical questions, particularly regarding the delegation of life-and-death decisions to machines. As previously discussed, (Marsili, 2023a), military disruptive technologies, including autonomous weapon systems, create a significant risk of delegating life-and-death decisions to machines without adequate ethical oversight. This raises profound ethical implications about whether machines can truly adhere to moral principles and whether humans should entrust such decisions to algorithms. This concern has been further explored by Marsili (2024), who applies the Autonomy Spectrum Framework to real-world systems, highlighting the legal and ethical dilemmas posed by delegating lethal decisions to autonomous technologies.

As these systems become more capable, they challenge traditional notions of human agency in warfare. Autonomous weapons, which can identify, select, and engage targets without direct human intervention, introduce complexities in accountability and proportionality, requiring a new ethical approach (Marsili, 2025a), two key principles of international humanitarian law (Crootof, 2018; Sharkey, 2019). The primary concern is that, while LAWS may enhance operational efficiency, they may also erode the human element in warfare, increasing the risk of violations of human rights (Sharkey, 2019).

In response to these challenges, scholars argue that the ethical use of LAWS requires more than just adherence to existing legal frameworks; it requires the development of an ethical resilience within military strategies (Anderson & Waxman, 2017). This involves integrating ethical considerations into the design, deployment, and usage of LAWS, ensuring that these systems operate in a way that respects human dignity and comply with the principles of international law (Scharre, 2018). The application of human rights in defence strategies, therefore, demands that states and international actors carefully consider the implications of technological advancements and establish robust safeguards to prevent abuses.

John Ruggie's concept of social purpose within the framework of business and human rights also provides valuable insight for the military context. Ruggie argues that businesses must respect human rights and ensure that their operations do not cause harm, a principle that can be

extended to the defense sector (Ruggie, 2011; 2013). This notion of social purpose in military technologies suggests that defence capabilities must not only be designed for strategic superiority but must also serve the broader goal of safeguarding human dignity and minimizing harm.

As military technologies evolve, too must the strategies that govern their deployment. The integration of human rights into defence capabilities is not merely a legal obligation but a necessary ethical practice, particularly in light of recent developments in AI and digital autonomy (Marsili, 2025b). The military sector must build ethical resilience to adapt to the changing landscape of warfare, ensuring that new technologies such as LAWS do not undermine international legal standards or infringe upon fundamental human rights (Marsili, 2022; Scharre, 2018).

Another critical factor shaping ethical decision-making in defence is the cultural relativity of how societies perceive acceptable military casualties. While democratic states may be constrained by political and public intolerance toward high loss of life, authoritarian regimes may be more willing to accept—or even conceal—substantial losses in pursuit of tactical objectives. This divergence in ethical calculus has profound implications for the implementation of human rights standards in asymmetric or hybrid conflicts.

Legal and Ethical Implications of Lethal Autonomous Weapons Systems

The deployment of autonomous weapons systems in modern warfare raises profound legal and ethical challenges, particularly regarding compliance with international humanitarian law [IHL] and international human rights law [IHRL]. LAWS—systems capable of independently identifying, targeting, and engaging military objectives—threaten to alter the nature of warfare, introducing new concerns about accountability, proportionality, and distinction between combatants and civilians (Crootof, 2018).

There are legal obligations and ethical considerations associated with the use of LAWS in military operations, as well as broader implications for human rights and ethical resilience. International humanitarian law, particularly the *Geneva Conventions* and their *Additional Protocols*, governs the conduct of warfare and aims to minimize the suffering of those involved in or affected by armed conflict. These principles require that all military actions comply with the core tenets of distinction, proportionality, and necessity (Scharre, 2018). The principle of distinction demands that parties to a conflict distinguish between combatants and civilians, targeting only legitimate military objectives. However, the implementation of LAWS in warfare presents significant challenges to this principle, as these systems must be capable of distinguishing between lawful and unlawful targets under complex and dynamic battlefield conditions (Crootof, 2018). The autonomy of these systems raises concerns about the accuracy

and reliability of such distinctions, particularly when LAWS are deployed in complex environments where the identification of civilians and non-combatants becomes more difficult.

The principle of proportionality, which prohibits attacks that may cause excessive harm to civilians or the natural environment in relation to the anticipated military advantage, is similarly jeopardized by LAWS. For instance, the use of fully autonomous drones in complex urban environments—such as those hypothetically envisioned in future autonomous strike missions—raises serious concerns about the system's ability to assess proportionality in real time, particularly where civilians are intermingled with combatants (Sparrow, 2007; Human Rights Watch, 2012). Critics argue that LAWS, lacking human judgment and empathy, may struggle to make nuanced assessments of proportionality in rapidly evolving combat scenarios (Sharkey, 2019). As autonomous systems are increasingly integrated into military strategies, the capacity for humans to intervene in targeting decisions diminishes, leading to fears of disproportionate harm and the erosion of accountability.

Additionally, the challenge of accountability remains paramount in the discussion of LAWS. Under existing IHL frameworks, accountability for violations of international law, such as unlawful killings or war crimes, typically falls upon human actors, whether military commanders or political leaders. However, as decision-making shifts to machines, the responsibility for violations becomes increasingly opaque, raising questions about whether and how accountability can be assigned (Anderson & Waxman, 2017). While LAWS may operate within the confines of IHL, legal scholars argue that further clarification is needed regarding the responsibility of the human operators and commanders who deploy them (Crootof, 2018). This ambiguity has led to calls for new frameworks and specific regulations that address the unique characteristics of autonomous systems in warfare.

The ethical implications of LAWS extend beyond legal concerns, involving a broader discourse on the morality of delegating life-and-death decisions to machines. Marsili and Wróblewska-Jachna (2024) highlight how the rapid developments in AI technology, such as deep learning, have led to an increased pervasiveness and proliferation of misinformation through deep fakes. This calls for a focus on international standards and policy measures to enhance the trustworthiness of AI systems.

Ethical theorists have raised serious concerns about the potential erosion of human dignity and the accountability of military forces engaged in combat (Scharre, 2018). One significant ethical challenge is the potential loss of human control over the application of force, which has traditionally been viewed as essential to preserving the ethical integrity of military operations (Sharkey, 2019).

According to John Ruggie's framework on business and human rights, the ethical use of technology—whether in the business or military domain—requires that systems be designed

with human rights protection at their core, ensuring that these technologies do not lead to harm (Ruggie, 2011; 2013). By extension, in the military context, the use of LAWS must be balanced by ensuring that these systems respect the rights and dignity of civilians and combatants alike. This includes ensuring compliance with IHL, while also considering the broader humanitarian impact of deploying such systems in conflict zones.

Ethical concerns regarding autonomy in warfare are also reflected in debates surrounding the moral implications of 'killer robots'. Critics argue that by allowing machines to make life-and-death decisions, societies risk undermining the human capacity for empathy, which is often considered essential to ethical decision-making in warfare (Sharkey, 2019). While LAWS may be capable of executing military strategies with precision, they lack the ability to weigh the broader ethical consequences of their actions in the way a human commander might. This moral agency, which involves the capacity to reflect on the consequences of one's actions and adapt to the complexities of warfare, is a core argument against the development and use of fully autonomous weapon systems.

The growing integration of LAWS also prompts reflection on the ethical resilience of military institutions in adapting to such technologies. Ethical resilience entails the ability of military organizations to adapt their strategies, tactics, and operational frameworks to integrate advanced technologies without compromising human dignity or the principles of international law (Anderson & Waxman, 2017). Military leadership must engage in ongoing ethical reflection, ensuring that technological advancements are aligned with fundamental human rights and international humanitarian principles.

Emerging Technologies and Their Implications

Emerging technologies are rapidly redefining modern defence by blurring the boundaries of conventional warfare and introducing new operational domains. Artificial intelligence, autonomous weapons, and cyber capabilities not only enhance military effectiveness but also disrupt established norms governing accountability, human oversight, and the lawful use of force. These developments challenge the principles of proportionality and distinction, shifting the character of armed conflict and raising urgent questions about the adequacy of existing legal and ethical frameworks.

One of the most significant innovations is the development of autonomous weapon systems, which can select and engage targets without human intervention. As highlighted by Scharre (2018), LAWS have the potential to increase operational efficiency and reduce human casualties, but they also introduce risks such as accountability gaps, lack of human judgement,

and the possibility of malfunction or unintended escalation. Autonomous systems could, for instance, make decisions in high-stakes combat situations where human emotions, biases, and ethical considerations could play a crucial role. Scharre (2018) argues that the challenge lies in ensuring that these systems comply with international humanitarian law, particularly the principles of distinction and proportionality, which require that military operations distinguish between combatants and civilians, and avoid excessive harm to civilians relative to the military advantage gained. Marsili's paper on LAWS (2024) discusses how these autonomous systems pose serious ethical dilemmas around the dehumanisation of warfare and the need for robust legal frameworks to ensure accountability and human oversight drawing on the dynamic autonomy model to propose a flexible approach that calibrates machine autonomy based on contextual complexity and humanitarian risk. The contribution advocates for stronger international regulations to ensure LAWS are used in compliance with ethical standards. Similarly, Crootof (2018) highlights how LAWS could lower the threshold for initiating armed conflicts, especially when integrated with AI systems capable of analyzing vast amounts of data and making rapid decisions, thus increasing the speed of warfare and potentially reducing opportunities for diplomatic intervention.

Artificial intelligence, which underpins many of these autonomous systems, also introduces new dimensions to warfare. As Crootof (2018) discusses, the deployment of AI in warfare may inadvertently lower the threshold for conflict initiation and escalation, particularly in cyber warfare and remote combat scenarios. Complementing this perspective, Zweibelson (2025) argues for a reconceptualization of warfare itself, emphasizing the need to understand conflict as a dynamic, multi-domain phenomenon influenced by technological disruption and shifting geopolitical realities. The ease of using AI for offensive operations can make it more likely for states to engage in conflicts without fully considering the long-term humanitarian consequences. Additionally, AI-driven systems raise concerns about the opacity of decision-making processes, as these technologies may not be easily understandable to human operators, making it difficult to attribute responsibility for errors or violations of IHL (Marsili, 2023a).

Cyber capabilities are another emerging technology that significantly impacts modern warfare. While cyber operations can be used to enhance national security and disrupt enemy systems, they also pose risks to civilian infrastructure and human rights. Attacks on critical infrastructure such as power grids, healthcare systems, or communication networks could have devastating effects on civilian populations. Moreover, the anonymity and low-cost nature of cyber warfare make it a particularly attractive option for non-state actors and rogue states, further complicating the global security environment. As highlighted in the literature, cyber warfare lacks clear rules of engagement, which raises questions about the legality of certain actions under

international law, particularly when it comes to attacks that have a direct impact on civilians (Ruggie, 2011).

While emerging technologies offer significant advantages in terms of military effectiveness, their implications for human rights are profound. As warned (Marsili, 2022), there is a growing need for comprehensive frameworks that can balance technological advancements with respect for international human rights standards. The risks of using autonomous systems and AI-driven technologies in military contexts include not only violations of IHL but also potential abuses of power by authoritarian regimes, who could leverage these technologies for surveillance, repression, and control over populations. This underscores the importance of ensuring that the development and deployment of these technologies are guided by robust ethical considerations and international cooperation.

The importance of establishing ethical guidelines and frameworks for emerging technologies in defence is further emphasized in studies examining their broader impact. As scholars continue to investigate the intersection between emerging technologies and human rights, it is critical that their development and use in warfare be continuously assessed to ensure that they adhere to international norms. The potential for states to abuse technologies such as AI and autonomous weapons underscores the need for effective oversight and governance (Sharkey, 2019). Furthermore, international collaboration will be necessary to develop a shared understanding of how these technologies should be used, ensuring that ethical resilience is maintained even as technological capabilities evolve.

To summarise, while emerging technologies have the potential to enhance defence capabilities, they also introduce significant risks. The challenge is to navigate the fine line between leveraging these innovations for military advantage and safeguarding human rights and ethical standards. The rapid evolution of AI, cyber capabilities, and autonomous systems is reshaping the strategic and operational landscape of modern defence, presenting profound ethical and legal challenges. These technologies blur traditional boundaries of warfare, complicating accountability and the protection of human rights. As discussed earlier, concerns around proportionality, distinction, and human control are central to understanding their impact. Against this backdrop, the concept of ethical resilience emerges as a vital framework to guide the responsible development and deployment of these innovations. As we move forward, it is crucial that discussions around such technologies remain anchored in the broader imperatives of human dignity, accountability, and compliance with international law, ensuring that technological progress aligns with the fundamental principles that safeguard society.

The increasing complexity of modern warfare, particularly in hybrid environments, further complicates the application of international humanitarian law. Hybrid threats, including cyber operations, disinformation, and proxy warfare, challenge the enforcement of accountability and the protection of civilians. As recent conflicts have shown, state and non-state actors alike may deliberately exploit the legal and ethical constraints observed by democratic societies, perceiving them as operational weaknesses. This underscores the importance of developing ethical resilience not only in relation to technological systems, but also to evolving strategic doctrines (Kaldor, 2012).

Ethical Resilience in Defence Capabilities

As military technologies evolve, ensuring their ethical integration within national defence strategies is paramount. The concept of 'ethical resilience' refers to the ability to adapt military strategies to rapidly advancing technologies while maintaining a commitment to core human rights principles. This involves a multifaceted approach to not only managing risks but also fostering a culture of accountability and ethical decision-making within defence institutions. The development of autonomous weapon systems, artificial intelligence, and cyber capabilities presents a unique challenge in this regard, requiring careful consideration of how these technologies are regulated and employed in military contexts.

The importance of ensuring that these technologies are not misused or employed irresponsibly is highlighted by scholars such as Crootof (2018), who contend that LAWS could radically shift the traditional understanding of accountability in warfare. Without proper oversight, these systems could make autonomous decisions that violate established ethical norms, leading to unintended harm or violations of international humanitarian law. Furthermore, Scharre (2018) underscores the importance of maintaining human oversight in such systems, as human judgement remains crucial in interpreting the complex moral and legal dimensions of warfare—an issue also highlighted by Christian (2020), who warns that even the most advanced AI systems struggle to internalize nuanced human values and ethical reasoning.

The growing reliance on AI in military decision-making processes poses significant questions about autonomy, accountability, and responsibility. Marsili's proposal (2023a) emphasizes the importance of integrating human rights considerations into the development and deployment of emerging military technologies like AI and autonomous systems. This includes maintaining human oversight, establishing accountability mechanisms, and fostering international cooperation to regulate these technologies within the bounds of international law and human rights principles.

In scenarios where human operators are physically or mentally disconnected from decision-making, the ethical implications become even more pronounced. As Sharkey (2019) notes, the delegation of life-and-death decisions to machines challenges fundamental ethical and legal frameworks, including principles of proportionality and necessity, central tenets of IHL. Thus, ensuring ethical resilience requires continuous oversight and adaptation of IHL to account for new technologies that blur the line between human and machine decision-making.

The issue of ethical resilience is further compounded by the use of cyber warfare tactics. The growing use of cyberattacks as a means of conducting warfare or influencing the geopolitical landscape presents a challenge to traditional ethical and legal frameworks. As Marsili (2023b) discusses, cyber capabilities can affect civilian infrastructures, potentially violating principles of distinction and proportionality under IHL. The integration of these technologies must thus be accompanied by comprehensive frameworks that ensure compliance with human rights standards, with a focus on transparency and accountability.

In response to these challenges, international legal scholars such as Ruggie (2011) have emphasized the importance of guiding principles for the integration of emerging technologies in military contexts. His work on business and human rights stresses that all technological advancements, particularly those used in defence, must adhere to ethical standards that protect fundamental human rights, ensuring that the pursuit of technological and strategic advantages does not come at the expense of moral obligations.

This ethical framework should be considered not as a static set of rules but as a dynamic and evolving set of principles that adapt to new challenges and threats. As such, ensuring ethical resilience in defence capabilities involves not only adhering to established international law but also anticipating and addressing future ethical dilemmas posed by emerging technologies. The key lies in promoting a balanced approach—one that leverages technological advancements for national security while simultaneously safeguarding the rights and dignity of individuals affected by these developments.

Legal and Regulatory Frameworks for Ethical Resilience in Emerging Military Technologies

The integration of emerging technologies, particularly in the realm of autonomous weapons systems and artificial intelligence, necessitates a robust legal and regulatory framework to ensure ethical resilience. This framework should address not only the operational aspects of these technologies but also the broader ethical, legal, and humanitarian challenges they pose. A key component of this framework is the adherence to existing international laws such as international humanitarian law, international human rights law, and various arms control treaties. However, as

the nature of warfare evolves with these new technologies, there is an increasing need to adapt and potentially expand these legal frameworks.

One of the primary concerns regarding the deployment of LAWS is ensuring compliance with the core principles of IHL, which include distinction, proportionality, and necessity. These principles require that military operations must distinguish between combatants and non-combatants, that the force used in combat must be proportionate to the military objective, and that force must only be used when necessary. Scharre (2018) argues that LAWS could potentially undermine these principles by operating with minimal human oversight, leading to unintentional civilian harm or disproportionate use of force. To mitigate these risks, Scharre (2018) suggests that strict accountability mechanisms and ongoing human oversight are essential to maintaining compliance with IHL.

Moreover, the issue of autonomy in military technologies raises significant legal questions about responsibility and accountability. As noted by Crootof (2018), when LAWS operate autonomously, they blur the lines of responsibility for their actions. Traditional legal frameworks assume that human agents are responsible for the actions of military technologies, but with the increasing autonomy of these systems, it becomes unclear who should be held accountable in the event of unlawful or unethical actions. To address this, Crootof (2018) suggests that international law must evolve to explicitly account for autonomous systems, ensuring that their use is regulated and that clear chains of responsibility are established.

In addition to IHL, international human rights law plays a crucial role in ensuring that military technologies do not violate fundamental human rights, particularly the right to life, liberty, and security. The United Nations *Guiding Principles on Business and Human Rights* (Ruggie, 2011) provides a framework for ensuring that all actors, including military organizations, respect human rights in the context of technological development and deployment. These principles emphasize the need for companies and governments to ensure that technologies, such as LAWS and AI systems, do not contribute to human rights abuses, including unlawful killings or violations of privacy.

Ruggie's (2013) work on multinational corporations and human rights further highlights the responsibility of private actors, such as defense contractors, in ensuring that their technologies are developed and deployed in a manner consistent with international human rights standards. This responsibility extends to ensuring that AI and other autonomous technologies used in military contexts are designed to minimize harm to civilians and avoid violations of fundamental rights.

Finally, the rapid development of AI in warfare raises significant challenges in terms of arms control and regulation. The potential for AI to be weaponized, as discussed by Sharkey (2019),

presents new challenges in regulating military technologies. Sharkey (2019) suggests that a global ban on autonomous weapons might be an ideal solution, but the practicalities of such a ban are fraught with difficulties, including the potential for states to circumvent regulations by developing technologies in secret or for non-state actors to use them. Instead, Sharkey (2019) advocates for robust international agreements that focus on controlling the use of autonomous weapons and AI in military operations while ensuring that they are used in accordance with established legal and ethical standards.

Ultimately, the legal and regulatory frameworks that govern the use of emerging military technologies must evolve to address the unique challenges posed by LAWS and AI. These frameworks should ensure that the principles of IHL, human rights law, and international arms control are adhered to, while also promoting ethical resilience through oversight, accountability, and international cooperation.

Analysis of Current Challenges and Opportunities

The integration of emerging technologies in military defense systems presents both significant opportunities and formidable challenges. The rapid advancement of artificial intelligence, autonomous weapon systems, and cyber capabilities has led to new paradigms in warfare, while simultaneously raising complex ethical, legal, and strategic issues. These technologies promise enhanced military effectiveness, precision, and the ability to conduct operations in more dynamic and unpredictable environments. However, they also bring substantial risks, particularly in relation to the preservation of human rights, the accountability of decision-makers, and the potential for unintended consequences.

A major challenge in the adoption of emerging technologies in defense is the alignment of technological capabilities with existing legal frameworks, particularly international humanitarian law. The use of autonomous weapons systems, for example, introduces concerns about compliance with principles such as distinction (*the ability to differentiate between combatants and non-combatants*) and proportionality (*ensuring the response is proportional to the threat*). The introduction of AI-driven systems in military contexts further complicates accountability and transparency, raising questions about who is responsible in the event of a malfunction or misuse (Anderson & Waxman, 2017; Scharre, 2018). Legal scholars argue that while some autonomous systems could potentially adhere to IHL standards, ensuring compliance at the operational level is far from guaranteed.

The absence of universally accepted frameworks to regulate these technologies underscores the gap between rapid technological development and existing regulatory

mechanisms. Many international bodies and scholars are calling for preemptive regulation or even bans on certain types of autonomous weapons to prevent potential abuses (Sharkey, 2019). However, as Anderson and Waxman (2017) highlight, a blanket ban on AI in warfare could stifle technological progress and limit the potential military advantages that could arise from these innovations.

Human rights concerns are another critical dimension in the deployment of emerging technologies in defense. Autonomous systems, especially those capable of lethal force, pose risks to human dignity and could undermine the protection of civilian life. Technologies like AI-driven drones or robotic soldiers challenge the traditional notions of human oversight in lethal decision-making. Ruggie (2011; 2013) emphasizes the importance of a framework that ensures businesses (*or in this case, military contractors*) and governments adhere to human rights standards, aligning military innovations with principles of justice and the protection of human life.

As emerging technologies increasingly influence military operations, ensuring that these technologies respect international human rights standards are crucial. The development of AI-driven defense systems must consider not only the military objectives but also the broader societal implications of autonomous decision-making in conflict, including the potential for escalation or misuse in authoritarian regimes (Marsili, 2022). The challenge lies in designing systems that retain human oversight while enhancing operational efficiency.

Despite these challenges, emerging technologies also present strategic opportunities that could significantly alter the landscape of defense. AI, for instance, could provide a more accurate and faster decision-making process, improve military capabilities while reducing the risk to human soldiers. Autonomous systems could also enhance the ability to conduct operations in complex environments, such as urban warfare or in regions with high levels of contamination, where human intervention might be impractical or too dangerous (Crootof, 2018; Scharre, 2018).

In addition, the integration of cyber capabilities into military defense has the potential to revolutionize warfare. Cyber-attacks can disrupt enemy communications, disable critical infrastructure, or gather intelligence without the need for traditional kinetic operations (Marsili, 2023b). These capabilities could offer a significant strategic advantage in situations where traditional warfare methods are less effective or impossible to use. The challenge, however, remains in ensuring that these capabilities are used ethically and within the bounds of international law.

The primary opportunity lies in balancing technological advancements with ethical responsibility. As Scharre (2018) suggests, achieving a balance between military power and human rights is fundamental. Technologies must be developed with an awareness of their potential

consequences, ensuring that the deployment of autonomous and AI-driven systems does not erode the core ethical principles that govern warfare. To navigate these challenges, it is essential to establish clear ethical guidelines and regulatory frameworks that guide the development, deployment, and use of emerging technologies in defense.

Moreover, as emerging technologies continue to evolve, it is essential for policymakers and military leaders to adopt a proactive approach to ethical resilience. This involves anticipating the potential risks and designing systems that are adaptable to future challenges, ensuring that defense capabilities remain robust while safeguarding human dignity and rights.

The integration of emerging technologies into military defense systems offers significant opportunities to enhance operational efficiency and effectiveness. However, these advancements must be carefully balanced with the ethical, legal, and human rights considerations that underpin modern warfare. By addressing the challenges and opportunities outlined above, the international community can ensure that technological advancements in defense contribute to greater security without undermining the fundamental values that govern warfare.

Strategic Recommendations for Integrating Human Rights and Emerging Technologies in Defense

The integration of emerging technologies into military defense systems offers numerous strategic benefits but also presents significant ethical and operational challenges. In order to harness the potential of artificial intelligence, autonomous weapons systems, and other disruptive technologies while safeguarding human rights, it is essential to develop comprehensive strategies that balance technological advancement with legal and ethical obligations. As argued (Marsili, 2024), future international regulatory efforts must ensure meaningful human control, especially in high-risk scenarios where civilian protection is paramount.

One of the first steps in ensuring that emerging technologies are used responsibly in defense is the establishment of clear ethical guidelines and legal frameworks. These frameworks should be built on existing international humanitarian law and human rights law while adapting to the specific challenges posed by autonomous systems and AI. Anderson and Waxman (2017) argue that while a ban on autonomous weapons might be unrealistic, it is crucial to shape the development of such systems in ways that ensure compliance with IHL principles such as proportionality and distinction.

To guide this process, governments and international bodies must engage in multi-stakeholder dialogues, including defense experts, ethicists, human rights advocates, and policymakers. These discussions should focus on creating common standards that can be applied

globally, ensuring that the deployment of autonomous systems respects fundamental human rights and remains consistent with military ethics.

Despite the potential for AI and autonomous systems to improve military capabilities, it is vital to retain human oversight in decision-making processes, particularly in the use of lethal force. As Scharre (2018) suggests, human control is essential to ensure that military operations remain aligned with ethical norms and legal standards. This could be achieved through hybrid systems where AI assists decision-making, but final judgments are made by human commanders.

Moreover, accountability mechanisms should be put in place to track the actions of autonomous systems and their operators. These mechanisms could include real-time monitoring of AI behavior, transparent auditing processes, and clear lines of accountability for any actions that result in violations of human rights or IHL.

Given the global nature of technological advancements and the potential for emerging technologies to be deployed across borders, fostering international cooperation is essential. Ruggie (2011) stresses the importance of the "Protect, Respect, and Remedy" framework, which guides the actions of both states and private companies in ensuring respect for human rights. For defense technologies, this framework can help ensure that military applications do not undermine human dignity or violate the rights of individuals, especially civilians caught in conflict zones.

The proliferation of private military companies [PMCs] and the widespread use of proxy forces further erode the traditional understanding of state monopoly on legitimate force. These actors, often operating outside the scope of international law, engage in combat operations without the same legal or ethical obligations as regular armed forces. This fragmentation of responsibility complicates the attribution of violations and weakens enforcement mechanisms for human rights and humanitarian law (Singer, 2003).

International agreements should be pursued to establish common norms and standards for the use of autonomous and AI-driven systems in military operations. These norms could include restrictions on the development and deployment of fully autonomous lethal systems and encourage transparency in the use of AI technologies.

Another key recommendation is the integration of human rights considerations into military strategy and training. As technologies evolve, it is essential that military personnel are educated on the ethical implications of these technologies. Training should include scenario-based exercises where military operators learn to navigate the ethical dilemmas posed by autonomous systems, ensuring they understand their responsibilities under IHL and human rights law.

Incorporating human rights into military strategy is not just about compliance; it is also about ensuring that military operations contribute to long-term peace and stability. As Marsili (2023b)

points out, ethical military practices are essential not only for legal compliance but for maintaining the legitimacy of military operations in the eyes of the global community.

Finally, defense technologies should not only be developed with a focus on combat efficiency but also with the aim of preventing conflicts and de-escalating tensions. AI and autonomous systems can be used to improve intelligence gathering, enhance early warning systems, and support peacekeeping missions by reducing the need for human intervention in high-risk areas.

However, the development of such technologies must be approached cautiously. As Sharkey (2019) warns, the increased reliance on autonomous systems could lead to unforeseen consequences, such as the escalation of conflicts or the inadvertent targeting of civilian populations. Therefore, adaptive technologies should prioritize conflict prevention and de-escalation capabilities to ensure that military engagement remains a last resort.

The integration of emerging technologies in defense offers significant potential for enhancing operational capabilities and improving strategic outcomes. However, these technologies must be deployed in a way that upholds human rights and adheres to ethical standards. By establishing clear legal frameworks, ensuring human oversight, fostering international cooperation, and prioritizing human rights in military strategy, it is possible to create a defense system that is both advanced and ethically resilient.

Conclusion

In conclusion, integrating human rights principles within emerging defence technologies is essential for ensuring their ethical deployment. As military capabilities increasingly incorporate advanced technologies such as artificial intelligence and autonomous systems, it becomes crucial to maintain a balance between their operational advantages and the protection of fundamental human rights. Proactive frameworks that prioritize accountability, transparency, and international law can ensure these technologies are developed and used responsibly.

By embedding human rights into military technology development, we can mitigate risks like accountability gaps and the potential for disproportionate harm. Moreover, as the nature of warfare continues to evolve with technologies like AI, cyber capabilities, and hybrid warfare, decision-makers must consider both technological advancements and ethical standards. Ensuring that innovations in military capabilities align with human rights will be vital for maintaining global stability, peace, and security in the face of future challenges. Thus, fostering a defence framework that is both resilient and ethically sound is critical to navigating the complexities of modern warfare.

References

Anderson, K., & Waxman, M.C. (2013). *Law and Ethics for Autonomous Weapon Systems: Why a Ban Won't Work and How the Laws of War Can*. Stanford University, The Hoover Institution (Jean Perkins Task Force on National Security and Law Essay Series), American University, WCL Research Paper 2013-11, Columbia Public Law Research Paper 13-351. http://dx.doi.org/10.2139/ssrn.2250126.

Christian, B. (2020). *The Alignment Problem: Machine Learning and Human Values*. W.W. Norton & Company.

Crootof, R. (2018). Autonomous Weapon Systems and the Threshold of Armed Conflict. *International Law Studies, 94*, 210–249.

DeRouen, K., & Heo, U. (2007). *Civil Wars of the World: Major Conflicts since World War II (Vols. 1–2)*. ABC-CLIO.

Human Rights Watch. (2012). *Losing Humanity: The Case Against Killer Robots*. https://www.hrw.org/report/2012/11/19/losing-humanity/case-against-killer-robots

Kaldor, M. (2012). *New and Old Wars: Organized Violence in a Global Era* (3rd ed.). Polity Press.

Kalyvas, S.N. (2006). *The Logic of Violence in Civil War*. Cambridge University Press. https://doi.org/10.1017/CBO9780511818462.

Marsili, M. (2022). Hybrid Warfare: Above or Below the Threshold of Armed Conflict?. *Hungarian Defence Review* (*Honvédségi Szemle*), *150*(1-2).

Marsili, M. (2023a). Military Emerging Disruptive Technologies: Compliance with International Law and Ethical Standards. In Kalpokas, I., & Kalpokienė, J. (Eds.), *Intelligent and Autonomous: Transforming Values in the Face of Technology* (pp. 25-50). Value Inquiry Book Series (VIBS), Vol. 390. Brill. https://doi.org/10.1163/9789004547261_004.

Marsili, M. (2023b). Guerre à la Carte: Cyber, Information, Cognitive Warfare and the Metaverse. *Applied Cybersecurity & Internet Governance* (ACIG), *2*(1), 1–11. https://doi.org/10.60097/ACIG/162861.

Marsili, M. (2024). Lethal Autonomous Weapon Systems: Ethical Dilemmas and Legal Compliance in the Era of Military Disruptive Technologies. *International Journal of Robotics and Automation Technology*, *11*, 63–68. https://doi.org/10.31875/2409-9694.2024.11.05.

Marsili, M. (2025a). Emerging and Disruptive Technologies: Strategic Implications and Ethical Challenges of Dual-Use Innovations. *Strategic Leadership Journal. Challenges for Geopolitics and Organizational Development*, 1, 57–71. https://doi.org/10.5281/zenodo.15305895.

Marsili, M. (2025b). DeGen Artificial Intelligence: Challenges and Opportunities of AI Applications. *European Cybersecurity Journal* (ECJ), *10*(1), 67–80. https://doi.org/10.5281/zenodo.15198603.

Marsili, M., & Wróblewska-Jachna, J. (2024). Digital Revolution and Artificial Intelligence as Challenges for Today. *Media i Społeczeństwo*, *20*(1), 19–30. https://doi.org/10.5604/01.3001.0054.6506.

Ruggie, J.G. (2011). *Guiding principles on business and human rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*. New York, NY: United Nations. https://digitallibrary.un.org/record/720245?v=pdf.

Ruggie, J.G. (2013). *Just Business: Multinational Corporations and Human Rights*. W.W. Norton & Company.

Scharre, P. (2018). *Army of None: Autonomous Weapons and the Future of War*. W.W. Norton & Company.

Sharkey, A. (2019). Autonomous Weapons Systems, Killer Robots and Human Dignity. *Ethics Inf Technol*, *21*, 75–87. https://doi.org/10.1007/s10676-018-9494-0.

Singer, P.W. (2003). *Corporate Warriors: The Rise of the Privatized Military Industry*. Cornell University Press.
Weinstein, J.M. (2007). *Inside Rebellion: The Politics of Insurgent Violence*. Cambridge University Press. https://doi.org/10.1017/CBO9780511808654.
Zweibelson, B. (2025). *Reconceptualizing War*. Helion & Company.

Chapter 2: Approaches to Assess Troop's Resilience in Defense

Col. Dr. Oleksandr **Maistrenko**, ORCID: https://orcid.org/0000-0002-9900-5930

"Give me a place to stand on, and I will move the Earth"- Archimedes of Syracuse.

Abstract:

Resilience is a term that has many meanings in various fields, both humanitarian and purely technical. This sometimes leads to a misunderstanding of the approaches used to assess resilience itself and its impact on the outcome of the operation (*action*). Moreover, the meaning of the term resilience in the military sphere also varies. Therefore, this study offers an attempt to generalize the meaning of the term resilience in the military sphere. An important question regarding defense resilience is the definition of its components. Defense resilience is proposed to be determined directly based on the components of combat power, in particular, conceptual, physical, and moral. Ensuring the resilience of each of these components will ensure the overall resilience of the defense. The components of resilience, based on the adopted concept, can include conformity and adaptability of doctrines, readiness and technology of troops, and moral and psychological readiness of personnel. Here, doctrinal compliance means the ability to take into account modern challenges on the battlefield by existing doctrinal documents. The adaptability of doctrines means the ability to adjust doctrinal documents to new challenges in the shortest possible time. The readiness of the troops means the ability to conduct combat operations, taking into account the number of personnel, their training, and the availability of weapons, equipment, and ammunition. Technology is understood as a characteristic of the level of technologies used to ensure resilience of defense. Moral and psychological readiness of the personnel is the ability of the personnel to perform combat tasks taking into account the moral orientations of the conflict, psychological resilience, and communication both within the armed forces and externally. This is a generalized division of defense resilience components that needs further detailing. It should also be noted that a more detailed consideration of these components and their clustering will allow us to more accurately determine the factors that affect resilience. The next problem proposed for consideration is the formalization of resilience through certain evaluation indicators (*criteria*). The essence of the problem is that resilience is very difficult to formalize because these indicators are usually interdependent. This makes it necessary to take into account certain correlation effects. However, it is difficult to determine the exact values of correlation moments, especially without practical verification. Therefore, the study proposes to identify resilience assessment indicators and possible correlation effects between them. Given the nature of resilience, the general indicators that will allow us to evaluate it are the intensity and probability of performing combat

tasks. That is, a comparison of these indicators for one's troops and the enemy's troops will make it possible to assess the real possibilities for ensuring resilience defense.

Keywords: Resilience, Ukraine, Israel, Military, Armed Forces

Introduction

Even the world might be fragile if you make enough effort; not to say about groups of troops. However, I don't think there's anyone wishing and having the possibility to overturn the Earth. At the same time, weakening a group of troops' resilience is a real problem. This is especially confirmed by recent events in Ukraine and Israel.

Inability to take into account troops and people's resilience at the beginning of active actions led to unexpected results both in Ukraine and in Israel. Inability to take into account the resilience of the Armed Forces, society, and the state as a whole caused the disruption of the plans of the Russian Federation. Despite the fact that comparison of the potentials of Russia and Ukraine shows a significant advantage of Russia, Ukraine demonstrates, if not superiority, then at least parity. This shows that the existing approaches to assessing both military and economic potentials are imperfect, regarding the resilience of both the country and separate groups of troops. That is, the problem is a weak connection between the existing techniques for assessing potential and real situation with resilience.

Another example of the importance of resilience in warfare is the Israel–Hamas War 2023. During this armed confrontation, it was demonstrated that even a resilient defense has its weak points. At the same time, regardless of the suddenness and unexpected methods of conducting the offensive, it was the resilience of the troop groups that allowed not only to prevent more significant consequences, but also to respond in the shortest possible time. This example shows that ensuring resilience at all levels allows you to neutralize the negative consequences of unexpected actions of the enemy.

Therefore, consideration of resilience during the planning of hostilities is not only desirable but also a necessary element, which is provided for by many doctrinal documents. Thus, in *AJP-3.2 ALLIED JOINT DOCTRINE FOR LAND OPERATIONS 2022* resilience is mentioned in many sections, in particular when defining the meaning of armed conflict and describing Security in Section 3 in *Chapter 1 – The operating environment*. In *Section 1 – Fighting Power* in Chapter 2 there is a mention of the cognitive resilience of the troops when they face fear and violence. Also, in *Section 5 – Interaction with other components*, resilience is listed as one of the attributes. Also in the same Section 5, it is said about resilience to threats from cyberspace. In *Section 3 – Joint*

Action and the Joint Functions in the Land Environment, Chapter 3 talks about resilient Command and Control [C2] and determines that resilience is one of the fundamental elements of force protection (AJP-3.2, 2022).

AJP-5 ALLIED JOINT DOCTRINE FOR THE PLANNING OF OPERATIONS 2019 also mentions resilience. In particular, one of the principles of war states that security demands resilience. Also, when defining the tasks of Civil-military cooperation [CIMIC], it is necessary to take into account national resilience to determine its impact on the achievement of the commander's objectives. (AJP-5, 2019).

Resilience is also mentioned many times in the 2016 Combat Charter of the "*Mechanized and Tank Troops of the Ground Forces of the Armed Forces of Ukraine*". *Section 2.2. Preparing for a Defensive Battle*, is about the need to ensure the resilience of the defense in preparing for a battle. In *Section 3. Offensive Battle*, it is said that it is necessary to take into account the resilience of the enemy's defense. Communication resilience and psychological resilience of servicemen is also mentioned in this charter. (Combat Charter, 2016).

It is clear that this is far from an exclusive list of doctrinal documents where resilience is mentioned. However, these documents clearly demonstrate, on the one hand, the importance of resilience, and on the other hand, the lack of clear approaches to determining the value of resilience in relation to any aspects. Thus, there was a certain discrepancy between the need to take into account resilience during operations planning and the lack of an opportunity to determine the value of this resilience. In other words, the main problem of the practical plan is the discrepancy between the need to consider resilience as one of the key categories of success in the operation and the impossibility of doing so. This is due to the lack of sustainable approaches to taking resilience into account when planning operations.

The Purpose and Objectives of the Study

Therefore, the purpose of the article is to develop a possible approach to assessing a group of troops' resilience in defense to take into account when planning operations. The main tasks when developing a possible approach to assessing a group of troops resilience in defense are:

- analysis of the existing definitions of the "resilience" category and formation of the definition taking into account the specifics of the combat use of the troop group;
- identification of resilience components (decomposition) by the homogeneity of processes (objects) when determining the nature of resilience;

- identification of factors that affect resilience, taking into account the characteristics of the components of resilience and determining the place of resilience in the structure of interconnected properties of the functioning of a group of troops;
- determination of indicators (criteria) for assessing a group of troops resilience in operations;
- determination of possible methods for assessing a group of troops resilience in operations and formalization of the process of sustainable functioning itself.

Analysis of the Existing Definitions of the "Resilience" Category

Moving on to the **first task of the research**, it should be noted that the category "resilience" is used in many areas and has many different definitions. However, all these definitions have common features and can be used to form a definition of the defense resilience of a troop group. Regarding the fields of application, resilience is found in many meanings, including 'climate resilience' (Bäckstrand & Lövbrand, 2015), disaster resilience (Cutter, 2016), seismic resilience (Bruneau, 2006), military resilience (*psychological resilience*) (Simmons & Yoder, 2013), resilience (*in engineering*) (Francis & Bekera, 2014). However, more interesting are studies that consider resilience as a property of complex sociotechnical systems, that is, systems related to both the human and technical components. So, in the study "*RESILIENCE*" by Kevin Grove, there is resilience:

> "the capacity over time of a system, organization, community or individual to create, alter, and implement multiple adaptive actions in the face of unpredictable climatic changes" (Grove, 2018).

According to this definition, resilience is the adaptation of one's functions to conditions, that is, the preservation of functions to achieve certain goals. However, the specified definition focuses more on adaptation to unforeseen challenges and does not directly indicate the achievement of the set goals. This definition allows for a change in the ultimate goals of the system to preserve its internal integrity, which in a way better describes adaptability, that is, the ability to adapt to challenges. A similar definition was proposed in the report "*Basic Patterns in How Adaptive Systems Fail*", in particular

> "Resilience is the systemic capacity to change as a result of circumstances that push the system beyond the boundaries of its competence envelope. The system may have to amend some, or even all its goals, procedures, resources, roles, or responsibilities. As a

> result of those changes, the work system then expresses a revised competence envelope. In effect, it becomes a different system" (Woods & Branlat, 2011).

The analysis of the proposed definition shows that the system can change during the adaptation of the system to challenges. Then the question arises, what is the criterion for maintaining the internal integrity of systems so that it is possible to claim that the system is stable? After all, under the influence of external factors, the system can change in different ways, keeping one of the categories unchanged, in particular, control, ultimate goals, functions, etc. Which of these systems can be called stable? Perhaps the system that kept control over changes in structure, functions, and ultimate goal? Or perhaps the system that can achieve the ultimate goal? Or, perhaps, the system that kept the parameters of its functions within the established norms? Another interesting definition of resilience in the work "*Measuring Resilience*", in particular

> "Resilience is a key feature of success in emerging complex sociotechnical systems. Resilience is achieving a new state of stability in a parameter space" (Hoffman & Hancock, 2017).

This definition is shorter, but it gives an understanding that resilience can have different criteria, but common to all criteria is ensuring the stability of the system in the space of variable parameters. Another short definition is an example from the Cambridge Business English Dictionary, in particular

> "Resilience is the quality of being able to return quickly to a previous good condition after problems" (Cambridge Business English Dictionary, 2011).

As well as definitions from the Merriam-Webster.com Dictionary:

> "Resilience is the ability of a body to regain its original size and shape after being compressed, bent, or stretched" (Merriam-Webster Dictionary, n/d).

These definitions show that another feature of resilience is the ability to return to the previous position after a change in structure and functions. This is an important feature that shows the difference between resilience and adaptability. However, this does not provide an answer to the question regarding the criterion for ensuring the resilience of the system. Some definitions of resilience from mathematics, in particular from the theory of solving nonlinear differential equations:

> Resilience according to Poincaré: "we have a state of equilibrium in which the system is. At a moment of time, the system is removed from this state and remains on its own. If the system returns to equilibrium, then the equilibrium is stable" (Kolyanova, 2016).

Resilience according to Lyapunov: “the state of the system is considered stable if, with some initial disturbances, the system remains in a certain neighborhood of the equilibrium state” (Kolyanova, 2016).

Resilience according to Lagrange: “is interpreted as the limitation of trajectories, that is, the system should not go beyond a certain area” (Kolyanova, 2016),

In general, these definitions describe the states of the system that meet various criteria of the internal integrity of the system and generally do not give an answer as to which definition could be used for the grouping of troops. The following definition is offered in the DOD Dictionary of Military and Associated Terms, in particular:

“Resilience – the ability of an architecture to support the functions necessary for mission success with higher probability, shorter periods of reduced capability, and across a wider range of scenarios, conditions, and threats, in spite of hostile action or adverse conditions. Resilience may leverage cross-domain or alternative government, commercial, or international capabilities” (DOD Dictionary, 2017).

In this definition, the criterion of internal integrity is specified, in particular, it is the preservation of functions, moreover, it is emphasized that the preservation of functions is necessary for the achievement of mission success. However, this definition itself does not say within what limits system functions should be preserved. Therefore, the results of the analysis show that the main problem of the proposed definitions is the vagueness and blurring of the criteria for determining the internal integrity of the system. Another problem is the lack of a clear distinction between resilience and adaptability, which makes it difficult to understand the essence of this category.

Based on the above, in the opinion of the author, an appropriate definition of a group of troops' resilience is one that separates this resilience from the general category and describes the peculiarities of the group's troops' functioning. So, a group of troops' resilience in defense is a property of the group that describes the ability of the group to function under the influence of negative factors, both internal and external, especially the influence of the enemy. The aforementioned ability of the grouping to function is determined by maintaining the functions of the grouping within the set limits, and when going beyond these limits, returning to the set range in the shortest possible time. The main criterion for preserving the internal integrity of the system, which indicates its resilience, is the achievement of the goal of the operation. The proposed definition makes it possible to proceed to **the identification of defense resilience components**

(*decomposition*) based on the homogeneity of processes (*objects*) when determining the nature of resilience.

Identification of Resilience Components (Decomposition)

Resilience, as a complex property, needs to be decomposed according to a certain characteristic for more accurate identification of its essence and determination of indicators for its evaluation. For further research, three known components of fighting power, in particular conceptual, physical, and moral (AJP-3.2, 2022), are proposed as a sign of resilience decomposition. It is clear that ensuring the resilience of each of these components will ensure the overall resilience of the defense. However, it is necessary to detail the essence of resilience with respect to each of the components. In general:

> "Conceptual component is the force's knowledge, understanding and application of doctrine, and its continuous learning and adaptation. It includes understanding the situation and the operating environment. For a multinational force, this component will also include doctrinal aspects of interoperability" (AJP-3.2, 2022).

So, based on this definition, resilience in terms of a conceptual component should describe both knowledge, understanding, and application of doctrine and their adaptation. That is, defense resilience is determined primarily by the quality of doctrines (Fedorchak, 2024). The more relevant the content of doctrines is to modern conditions and the more adapted doctrines are to taking into account new experience, the more stable the defense will be. Thus, it can be argued that one of the components of defense resilience is compliance and adaptability of doctrines. Regarding the physical component, it should be noted that this component is the most understandable in relation to resilience because it refers to the physical (*comprehensible*) plane of combat power. Yes, according to *AJP-3.2 ALLIED JOINT DOCTRINE FOR LAND OPERATIONS*:

> "The physical component consists of the correct mix of personnel, equipment, training, sustainment and readiness. It is very much a quantitative, measurable component" (AJP-3.2, 2022).

Consideration of this component shows that the main criteria for ensuring defense resilience are the readiness of the group to conduct hostilities, in particular, the availability of personnel and equipment necessary to perform the assigned tasks. It is also necessary to note the preparation of the troops for the execution of tasks, which includes training and providing support to the troops during the execution of tasks (Henåker, 2022). Another important element of ensuring resilience is the appropriate level of technology, which corresponds to the ability to

counter the enemy's technology. When discussing the physical resilience of a force, one must consider how well the command and control [C2] system works. In real-world operations, a unit's ability to recover under pressure is closely tied to how smoothly and effectively it is led. The C2 system involves keeping everyone working together in the right rhythm and ensuring that troops and equipment are where they need to be, when they need to be. That's why strong C2 is vital to the physical resilience of a force. Based on the above, the defense resilience component in the context of the physical component is the readiness and technology of the troops. Next is the moral component. General definition according to *AJP-3.2 ALLIED JOINT DOCTRINE FOR LAND OPERATIONS:*

> "The moral component is the ability to get people to fight and operate and to do so appropriately. It comprises the force's morale, leadership and ethical conduct, along with the unique culture of that force" (AJP-3.2, 2022).

The analysis of this component shows that the resilience of the defense depends significantly both on the moral ability of soldiers to conduct combat operations and on the psychological readiness of commanders to make the right decisions in a difficult situation. The peculiarity of this component lies in the difficulty of formalizing the magnitude of its impact on defense resilience. Moreover, this component changes most dynamically during hostilities and is influenced by a large number of factors (Weissmann & Nilsson, 2023). Therefore, this component of defense resilience can be labeled as the moral and psychological readiness of the troops.

Identification of Factors that Affect Resilience

Thus, the main components of defense resilience, based on the accepted concept, can be attributed to compliance and adaptability of doctrines, readiness and technological capability of troops, and moral and psychological readiness of troops. The next task of the research is to **identify the factors** that affect the resilience of the defense, taking into account the characteristics of its components and determining the place of resilience in the structure of the interconnected properties of the functioning of the army group. Analysis of recent military conflicts has shown that defense resilience depends on many factors, but we can single out a few that have gained special importance recently. First of all, this is the goal of the operation, based on the accepted definition, the goal of the system's functioning is the criterion for determining the internal integrity of the system. Example: the withdrawal of Ukrainian troops from Avdiyivka in February 2024, (Radio Svoboda, 2024), in particular, the purpose of the units that came to reinforce was to ensure the holding of positions for a certain time, to ensure the withdrawal of the main forces. It was the

definition of a clear, understandable, and achievable goal that ensured the moral component of the combat force, in particular, the moral and psychological readiness of the troops to perform the task. This example shows the relationship between the effectiveness of the troops and their resilience functioning.

The next important factor is the availability of technology, and it should be noted that the availability of technology is considered not only in the military aspect. That is, access to various technologies provides an increase in both the resilience of functioning (*better protection, identification of objects, etc*.) and the efficiency of task performance. On the one hand, efficiency increases due to better opportunities to destroy enemy objects, on the other hand, better protection allows you to preserve troops and extend the time of their combat-ready functioning.

An example of the influence of this factor is the use of drones, mobile electronic devices, and mobile Internet (*Starlink*) (Berezhnyi & Trystan, 2023). In general, the analysis of this factor shows the interconnectedness of resilience and the effectiveness of functioning. The next important factor related to the conceptual component of combat power is the speed of introduction of new procedures, weapons designs, and tactics. Directly, the speed of implementation allows you to level the advantage in the combat power of the enemy, increasing the effectiveness of the execution of tasks. The same example is the creation of a new kind of troops - the Forces of unmanned systems in the structure of the Armed Forces of Ukraine (Decree of the President of Ukraine, 2024).

Along with these factors, other factors remain relevant, such as combat capabilities, the number of forces and consumption of resources and forces attrition in combat (Kostić & Jovanović, 2023), military climate and discipline (Bester & Stanz, 2007) and different approaches to factor evaluation are used, for example, Critical Factors Analysis (Helmick, 2004). However, it should be noted that the factors considered above make it possible to determine the place of resilience in the structure of the interconnected properties of the functioning of a group of troops.

Thus, based on the analysis, the main properties are the performance, efficiency, and resilience of the functioning of the troop group. Here, efficiency is understood as the ability of a group to achieve its goals taking into account costs (*losses*), in other words, efficiency is the degree of realization of the capabilities of a group of troops (Maistrenko et al, 2021a). Performance here is understood as the group's ability to obtain a result in a certain period of time and at the set costs (*losses*) (Maistrenko et al, 2021b). And, according to the definition adopted within this study, resilience is the ability of a group to function under the influence of negative factors, both internal and external, especially the influence of the enemy.

Based on these definitions and the analysis of the most important factors that affect the operation, it can be argued that efficiency is a complex property that reflects the overall degree of goal achievement. Moreover, performance and resilience are components that reflect different aspects of effectiveness. Thus, performance reflects the potential ability to perform tasks, and resilience reflects the actual ability to perform tasks under certain conditions. It is also necessary to note the interconnectedness of performance and resilience. Thus, performance affects resilience through its impact on the enemy's combat capability, and resilience affects performance through its impact on the combat capability of its own troops. This interrelationship is clearly demonstrated by an example. Let's imagine two sides that have the same set of forces and means enter into a combat clash. It is clear that each of the parties will try to inflict maximum damage on the enemy, but the use of a large number of means of destruction will lead to a greater probability of their detection and damage by the enemy and, accordingly, a decrease in resilience. At the same time, using a large number of means of destruction can lead to a higher probability of hitting enemy targets, which will increase performance.

Determination of Indicators for Assessing a Group of Troops' Resilience in Operations

Thus, a logical dilemma arises when increasing performance, we decrease resilience, and when increasing resilience, we decrease performance. This determines the consideration of both properties as a whole without limiting one of them. Moreover, it once again confirms the importance of resilience research. The study of the interrelationship of the properties of the grouping allows us to move on to the determination of **indicators (*criteria*)** for assessing a group of troops resilience in operations. Based on the definition of the indicator, in particular:

> *"indicator* – in the context of assessment, a specific piece of information that infers the condition, state, or existence of something, and provides a reliable means to ascertain performance or effectiveness" (JP 5-0, 2020).

The indicator should reflect the degree of achievement of this or that effect. In general, the set of indicators should fully show the extent to which the potential opportunities of the grouping were / can be realized. Considering the nature of the combat conflict process, it is possible to single out several important factors that significantly affect resilience and performance. First of all, this is a high degree of uncertainty when evaluating processes, this is due to a large number of factors that influence each other and the competitive nature of the interaction of the opposing parties. That is, in other words, the vast majority of the results of the functioning of these parties are probabilistic in nature. Taking this into account, an important group of indicators when

evaluating the properties of a grouping in operations are the probabilities of the occurrence of this or that event.

The next important factor is the number of actions (*tasks*) that the parties can perform in a certain period of time. This is explained by the fact that the interaction of the opposing parties is based on the repetition of certain actions depending on the functional affiliation of the executive system. In other words, the entire interaction of the parties is based on repeated repetition of the same type of actions. For example, fire from a cannon, return of combat commands, reconnaissance of targets. In view of the above, an important group of indicators for evaluating grouping in operations is the intensity of task performance, that is, their frequency (*number per unit of time*).

Another important factor that affects the effectiveness of the combat use of the group in operations is the ability to inflict damage on the enemy. This is a very complex factor, because the damage can be measured both by material parameters, such as the number of losses of personnel and weapons, and by non-material ones - a decrease in morale, disruption of communication channels, etc. However, it should be noted that each of these tasks is characterized by a certain weight, that is, the amount of influence on the result of the operation. For example, the importance of carrying out several tasks to defeat the enemy's manpower in order to suppress them is equal to one task to destroy the point of overcoming tactical barriers (*a bridge across a river, tunnels (passes) in the mountains, etc.*). That is, the next group of indicators is the importance of tasks (*objects*).

It should be noted here that there are many approaches to determining importance, but it is necessary to pay attention to two fundamentally different approaches. First, it is a determination of the importance of the tasks that the parties can perform. This approach is based on the distribution of the potential ability to perform tasks among the available means and, subsequently, the determination of the ability to realize these capabilities. The second approach is based on determining the importance of objects. This approach describes the potential contribution of each object in obtaining a certain result (*fulfillment of tasks*). Both of these approaches have their advantages and disadvantages, but within the same study it is advisable to follow one of them to avoid double counting of exposure effects.

Therefore, the main groups of indicators that could fully describe the armed confrontation of the parties can be the probability and intensity of task performance and the importance of these tasks (*objects*). However, it is necessary to take into account that the indicators reflect only a certain side of the process. For an objective comprehensive assessment of the process, it is necessary to determine the interrelationship between these indicators.

One of the main obligations of the proposed evaluation indicators is the connection between the functioning of one party and the other, because their functioning is aimed at maximizing the influence on the other party and minimizing it on its own. Therefore, it can be concluded that the indicated indicators are directly related, but with different signs. For example, the probability of completing the task of hitting an enemy object is directly related to the probability of hitting this object. That is, in other words, we can say that the performance evaluation indicator of one party is the inverse of the resilience evaluation indicator of the other party. In general, this interrelationship can be represented by dependence:

Figure 2.1: *An equations that reflects the interrelationship between the resilience and performance of two opposing sides*

$$\frac{F_1\left(\{P_i\},\{\lambda_i\},\{W_i\}\right)}{F_2\left(\{P_j\},\{\lambda_j\},\{W_j\}\right)} \square \quad \frac{F_2\left(\{P_j\},\{\lambda_j\},\{W_j\}\right)}{F_1\left(\{P_i\},\{\lambda_i\},\{W_i\}\right)},$$

where, $F_1\left(\{P_i\},\{\lambda_i\},\{W_i\}\right)$ – the objective function of the combat confrontation of the first party, taking into account the aggregates of probabilities $\{P_i\}$, intensities $\{\lambda_i\}$ performance of tasks by the first party and their importance $\{W_i\}$,

$F_2\left(\{P_j\},\{\lambda_j\},\{W_j\}\right)$ – the objective function of the combat confrontation of the other side, taking into account the aggregates of probabilities $\{P_j\}$, intensities $\{\lambda_j\}$ execution of tasks by the other party and their importance $\{W_j\}$.

Thus, the selection of a set of indicators for evaluating the properties of the group allows us to move on to the definition of possible **methods for assessing a group of troops' resilience** in operations and the formalization of the process of sustainable functioning itself.

Determination of Possible Methods for Assessing a Group of Troops' Resilience

There are many different approaches to modeling the armed confrontation process, including those based on Lanchester equations (Kress, 2020), queuing theory (Zhao et al, 2024), mathematical programming methods (Rahkar, 2020), game theory (Ho, 2022) and many others.

However, almost all of them are based on modeling the process of obtaining a result, i.e. performance with resilience as a limitation. Although taking into account the above, performance cannot be considered without taking into account the impact of resilience and vice versa. Therefore, the main task of further research is the selection of such an approach that would take into account the mutual influence of resilience and performance.

One of the interesting approaches to modeling the confrontation between opposing parties is the Lotka-Volterra equation (Malcai, 2002). These equations were first used to model the interaction of two animal populations, in particular predator-prey (Takeuchi et al, 2006), and later transformed to other variations: predator-predator (Morris & Pratt 2003), non-predator-non-predator (Bunin, 2017), etc. The advantage of these equations is that they allow us to directly take into account the performance-resilience relationship. Moreover, these equations make it possible to find the point of critical accumulation of damage (bifurcation point).

The point of critical accumulation of damage (bifurcation point) is the point where the system (one of the parties) loses equilibrium, i.e. resilience. That is, with the correct formalization of the input parameters in these equations, it is possible to simulate the loss of resilience of one of the parties, in other words, to determine the necessary conditions for achieving victory. Moreover, it is necessary to take into account that performance and resilience are mutually influencing properties. General view of the Lotka-Volterra equations:

Figure 2.2: *A system of Lotka-Volterra equations that reflects the mutual influence of two opposing sides*

$$\begin{cases} \dfrac{dN_1}{dt} = a_1 N_1(t) - b_1 N_1(t) N_2(t) - c_1 N_1(t)^2, \\ \dfrac{dN_2}{dt} = a_2 N_2(t) - b_2 N_1(t) N_2(t) - c_2 N_2(t)^2, \end{cases}$$

where, $N_1(t), N_2(t)$ – parameters that are subject to two-way forecasting, it can be the number of units, the number of tasks, etc;

a_1, a_2 – growth coefficients for two sides, which characterize the law of growth of the main forecasting parameter, i.e. performance;

b_1, b_2 – interaction coefficients, which characterize the law of mutual influence of the parties on each other, that is, the relationship between resilience and performance;

c_1, c_2 – coefficients of self-limitation, which characterize the law of conservation of resilience under the influence of internal factors.

To illustrate the approach, let's consider a model that describes the change in the intensity of combat tasks over time for our unit. where a_1 and a_2 are the rates of recovery of combat capabilities for each side; b_1 and b_2 are the intensity of losses during mutual impact; and c_1 and c_2 are "internal friction," which takes into account logistical difficulties and management constraints.

Calculation parameters:

$a_1 = 0.05$; $a_2 = 0.01$ (our unit has a higher recovery rate);

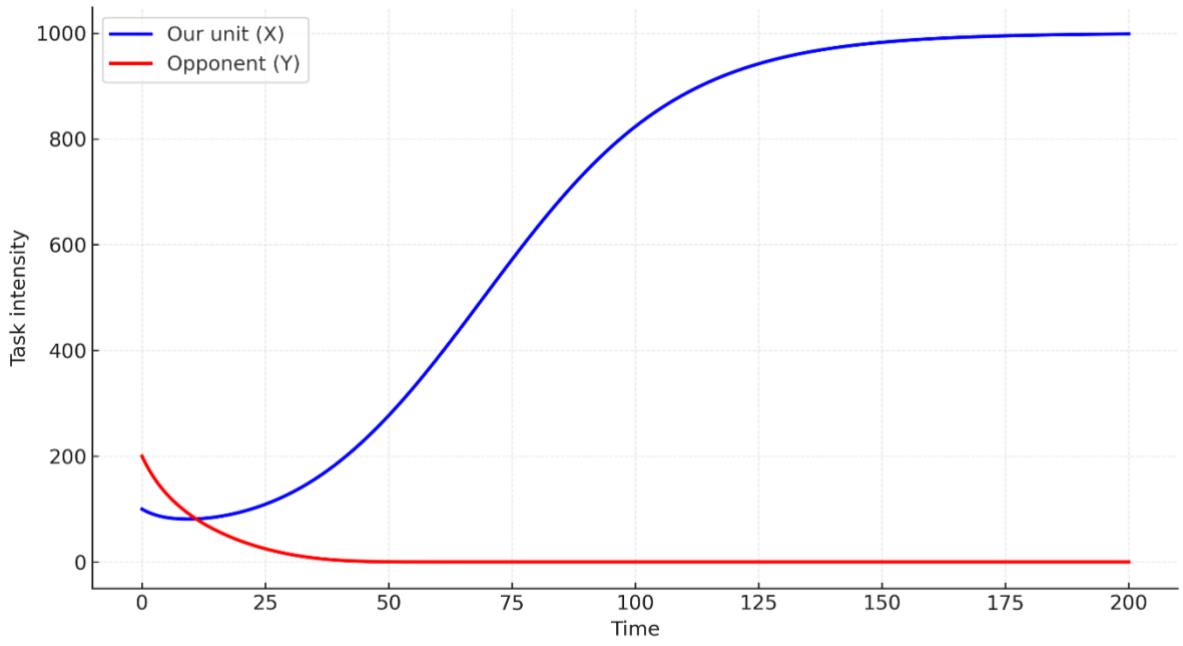
$b_1 = 0.0005$; $b_2 = 0.001$ (less losses upon contact for us);

$c_1 = c_2 = 0.00005$ (the level of internal "friction" is the same for both sides).

Initial conditions:

$N_1(0) = 100$; $N_2(0) = 100$ combat tasks per unit of time (i.e. the enemy has a quantitative advantage at the beginning).

Figure 2.3: *Dynamics of parameter changes with higher resilience of our unit (higher recovery rate and lower losses during combat interaction)*



Numerical simulations have shown that, due to the higher recovery rate and lower sensitivity to combat losses, our unit quickly increases the intensity of tasks and surpasses the enemy at approximately the 40th–50th hour of combat. After that, its activity stabilizes at a high level, while the enemy's activity gradually decreases.

This example emphasizes the interrelationship of resilience and effectiveness and also demonstrates the possibility of applying this approach to combat planning. The results obtained can be used to evaluate and compare scenarios in the operational planning process, as well as to develop recommendations for increasing the resilience and combat effectiveness of military groups.

Despite all the advantages of the proposed approach, it has not been widely distributed among research related to the simulation of combat operations, due to certain difficulties. One of the main difficulties is the difficulty of formalizing the coefficients of growth, interaction, and self-limitation. This is due to the fact that the determination of each of these coefficients requires the determination of indicators that would fully reflect the peculiarities of the process and the study of the laws of the functioning system. If the solution to the first question related to indicators is proposed in this study, then the second question related to the laws of functioning systems requires a more thorough study.

Despite the above difficulties, the general approach to modeling the process of armed conflict has the right to exist. Moreover, this approach makes it possible to comprehensively evaluate the resilience of the functioning (*defense*) of a troop grouping in an operation, taking into account the impact of performance, and to generally assess the effectiveness of this grouping in operations.

Conclusion

Thus, the report proposes a possible approach to assessing a group of troops' resilience in defense, which will be able to increase the accuracy of forecasting an armed confrontation to take into account when planning operations. It is also proposed to define the defense resilience category (*operational resilience*) of the troop group based on the analysis of the existing definitions of the "resilience" category and taking into account the specifics of the combat use of the troop group.The components of resilience have been identified in accordance with the components of fighting power (conceptual, physical, and moral), in particular, the compliance and adaptability of doctrines, the readiness and technological capabilities of the troops, the moral and psychological readiness of the troops.

It was determined that resilience is an interrelated property with performance and, in the complex, a component of the effectiveness of the functioning of a group of troops. It was found that the main groups of indicators for assessing a group of troops' resilience in operations are probability and intensity of task performance and the importance of these tasks (*objects*). A general approach to assessing a group of troops resilience in defense is proposed, which is based on the

complex consideration of the relationship with performance through the application of the Lotka-Volterra equations. The direction of further research considers the formalization of growth coefficients, interaction, and self-limitation through the study of the laws of the functioning of the group in operations.

References

Bäckstrand, Karin, ta Eva Lövbrand. 2015. *Research Handbook on Climate Governance*. Elgar Publishing Limited, Edward.

Berezhnyi, A., ta A. Trystan. 2023. "PREDICTING THE DEVELOPMENT OF THE TECHNOLOGICAL BASIS FOR THE WARS OF THE FUTURE". *Naukovi pratsi Derzhavnoho naukovo-doslidnoho instytutu vyprobuvan i sertyfikatsii ozbroiennia ta viiskovoi tekhniky*, 18, № 4: 122–35. https://doi.org/10.37701/dndivsovt.18.2023.17.

Bester, Piet C., ta Karel J. Stanz. 2007. "The conceptualisation and measurement of combat readiness for peace-support operations – an exploratory study". *SA Journal of Industrial Psychology*, 33, № 3 (19 bereznia). https://doi.org/10.4102/sajip.v33i3.398.

Bruneau, M., ta A. Reinhorn. 2006. "Overview of the resilience concept." U *8th US national conference on earthquake engineering*, 18–22. https://www.researchgate.net/profile/Andrei-Reinhorn/publication/265145848_Overview_of_the_Resilience_Concept/links/5733ba7108ae298602dcf04e/Overview-of-the-Resilience-Concept.pdf.

Bunin, Guy. 2017. "Ecological communities with Lotka-Volterra dynamics". *Physical Review E*, 95, № 4 (28 kvitnia). https://doi.org/10.1103/physreve.95.042414.

Cambridge business English dictionary. 2011. Cambridge: Cambridge University Press.

Cutter, Susan L. 2016. "Resilience to What? Resilience for Whom?" *Geographical Journal*, 182, № 2 (17 kvitnia): 110–13. https://doi.org/10.1111/geoj.12174.

"Definition of RESILIENCE". b. d. U *Merriam-Webster: America's Most Trusted Dictionary*. Data zvernennia 17 chervnia 2024. https://www.merriam-webster.com/dictionary/resilience.

Fedorchak, Viktoriya. 2024. *The Russia-Ukraine War: Towards Resilient Fighting Power*. Routledge. https://doi.org/10.4324/9781003351641.

Francis, Royce, ta Behailu Bekera. 2014. "A metric and frameworks for resilience analysis of engineered and infrastructure systems". *Reliability Engineering & System Safety*, 121 (sichen): 90–103. https://doi.org/10.1016/j.ress.2013.07.004.

Grove, Kevin. 2018. *Resilience*. Taylor & Francis Group.

Helmick, Jerry. 2004. *The Sequel to Major Combat Operations - Applying Critical Factors Analysis to OIF*. Fort Belvoir, VA: Defense Technical Information Center. https://doi.org/10.21236/ada426024.

Henåker, Lars. 2022. "Decision-making style and victory in battle—Is there a relation?" *Comparative Strategy* 41 (4): 415–36. https://doi.org/10.1080/01495933.2022.2087436.

Ho, Edwin, Arvind Rajagopalan, Alex Skvortsov, Sanjeev Arulampalam ta Mahendra Piraveenan. 2022. "Game Theory in Defence Applications: A Review". *Sensors*, 22, № 3 (28 sichnia): 1032. https://doi.org/10.3390/s22031032.

Hoffman, Robert R., ta P. A. Hancock. 2017. "Measuring Resilience". *Human Factors: The Journal of the Human Factors and Ergonomics Society*, 59, № 4 (30 sichnia): 564–81. https://doi.org/10.1177/0018720816686248.

Joint 7/Joint Doctrine Branch. 2020. *Joint Planning*. Joint Publication 5-0. Washington, D.C.: Joint Staff, J-5 Pentagon. https://irp.fas.org/doddir/dod/jp5_0.pdf.

Joint Chiefs of Staff Washington United States. 2017. *DOD Dictionary of Military and Associated Terms: As of November 2019*. Department of Defense (DOD).

Kolyanova, T. 2016. *DYNAMIKA POPULIaTsIINYKh SYSTEM*. Kyiv: KYIVSKYI NATsIONALNYI UNIVERSYTET IMENI TARASA ShEVChENKA. https://csc.knu.ua/media/filer_public/54/6f/546f1d79-e7f0-42d6-8e33-d90f39f4474a/dps_navch_pos.pdf#:~:text=Стійкість%20за%20Ляпуновим:%20стан%20системи,в%20певному%20околі%20стану%20рівноваги.

Kostić, Mladen, ta Aca Jovanović. 2023. "MODELING OF REAL COMBAT OPERATIONS". *Journal of process management and new technologies*, 11, № 3-4 (11 lystopada): 39–56. https://doi.org/10.5937/jpmnt11-46482.

Kress, Moshe. 2020. "Lanchester Models for Irregular Warfare". *Mathematics*, 8, № 5 (7 travnia): 737. https://doi.org/10.3390/math8050737.

Maistrenko, Oleksandr, Vitalii Khoma, Oleksandr Lykholot, Andrii Shcherba, Oleksandr Yakubovskyi, Stanislav Stetsiv, Alexander Kornienko ta Andrii Saveliev. 2021. "Devising a procedure for justifying the need for samples of weapons and weapon target assignment when using a reconnaissance firing system". *Eastern-European Journal of Enterprise Technologies*, 5, № 3 (113) (31 zhovtnia): 65–74. https://doi.org/10.15587/1729-4061.2021.241616.

Maistrenko, Oleksandr, Yevhen Ryzhov, Dmytro Khaustov, Sergiy Tsbulia ta Yuriy Nastishin. 2021. "Decision-Making Model for Task Execution by a Military Unit in Terms of Queuing Theory". *Military Operations Research*, 26, № 1 (berezen): 59–69. https://doi.org/10.5711/1082598326159.

Malcai, Ofer, Ofer Biham, Peter Richmond ta Sorin Solomon. 2002. "Theoretical analysis and simulations of the generalized Lotka-Volterra model". *Physical Review E*, 66, № 3 (6 veresnia). https://doi.org/10.1103/physreve.66.031102.

Morris, Steven A., ta David Pratt. 2003. "Analysis of the Lotka–Volterra competition equations as a technological substitution model". *Technological Forecasting and Social Change*, 70, № 2 (liutyi): 103–33. https://doi.org/10.1016/s0040-1625(01)00185-8.

NATO. 2019. *ALLIED JOINT DOCTRINE FOR THE PLANNING OF OPERATIONS*. NATO STANDARD AJP-5. NATO STANDARDIZATION OFFICE (NSO).

NATO. 2022. *NATO STANDARD AJP-3.2 ALLIED JOINT DOCTRINE FOR LAND OPERATIONS*. NATO STANDARD AJP-3.2. NATO STANDARDIZATION OFFICE (NSO).

Radio Svoboda. 2024. "Ukrainski pidrozdily vyishly z Avdiivky – Syrskyi". 17 liutoho 2024. https://www.radiosvoboda.org/a/news-avdiyivka-vyvedennya-syrskyy/32823485.html.

Rahkar Farshi, Taymaz. 2020. "Battle royale optimization algorithm". *Neural Computing and Applications*, 2 chervnia. https://doi.org/10.1007/s00521-020-05004-4.

Simmons, Angela, ta Linda Yoder. 2013. "Military Resilience: A Concept Analysis". *Nursing Forum*, 48, № 1 (sichen): 17–25. https://doi.org/10.1111/nuf.12007.

Takeuchi, Y., N. H. Du, N. T. Hieu ta K. Sato. 2006. "Evolution of predator–prey systems described by a Lotka–Volterra equation under random environment". *Journal of Mathematical Analysis and Applications*, 323, № 2 (lystopad): 938–57. https://doi.org/10.1016/j.jmaa.2005.11.009.

Ukraina. KOMANDUVANNIa SUKhOPUTNYKh VIISK ZBROINYKh SYL UKRAINY. 2016. *BOIOVYI STATUT "MEKhANIZOVANYKh I TANKOVYKh VIISK SUKhOPUTNYKh VIISK ZBROINYKh SYL UKRAINY"*. BOIOVYI STATUT SBP 3-(01,02,04).56(57). Ukhvaleno 30 hrudnia 2016.

Ukraina. Prezydent Ukrainy. 2024. *Pro naroshchuvannia spromozhnostei syl oborony*. Ukaz Prezydenta Ukrainy 51/2024. Ukhvaleno 6 liutoho 2024. https://zakon.rada.gov.ua/laws/show/51/2024#Text.

Weissmann, Mikael, ta Niklas Nilsson. 2023. *Advanced Land Warfare: Tactics and Operations*. Oxford University Press.
Woods, David D., ta Matthieu Branlat. 2011. "Basic Patterns in How Adaptive Systems Fail". U *Resilience Engineering in Practice*, 127–43. CRC Press. https://doi.org/10.1201/9781317065265-10.
Zhao, Wenfei, Kenan Teng, Jian Chen ta Yan Wang. 2024. "Research on operational effectiveness of air and missile defence in maritime stronghold based on queuing theory". *International Journal of Information and Communication Technology* 24 (2): 200–212. https://doi.org/10.1504/ijict.2024.137202.

Chapter 3: The legal challenges in the protection of submarine cable

Ahmed Abdel **Hakam**, ORCID: https://orcid.org/0009-0003-4781-2444

Abstract

Around 97% of international data traffic nowadays is actually routed through submarine fibre-optic cables, which form the backbone of global connectivity infrastructure (Sunak, 2017, p. 2; Submarine Telecoms Forum, 2025, p. 106). The security, stability, and resilience of these cables are crucial to ensure the continued operation of global communications and commerce. However, this critical piece of infrastructure is not exempted from global vulnerabilities and is still a system that is susceptible to the effects of natural disasters and disruption from State and non-State actors. International laws and conventions establish certain degrees of protection for these cables, but current international legal mechanisms fall short of responding to modern threats. A more substantial and more adaptive legal regime is needed to protect this critical piece of infrastructure, as geopolitical tensions, cyber vulnerabilities, and technological advances will continue to grow.

Keywords: Submarines, Submarine Cables, Communication, Hybrid Warfare

Introduction

In the 1850s, the first commercial submarine cable installation across the English Channel—making possible real-time telegraph communication between the United Kingdom and mainland Europe—altered the very fabric of global communication and brought the telegraph closer to people by dramatically decreasing transmission delays, paving the way for the technological and infrastructural transition that would ultimately culminate in the systems of telecommunications on which we now depend (Carter et al, 2009, p. 3; Harbin, 2021, p. 354). Today, submarine cables use advanced fibre-optic technology, encoding information into light waves sent by lasers through thin glass fibres, with throughput depending on the optical technologies used. The latest fibre links are able to handle over 200 terabits per second (Brake, 2019, p.1). In reality, the active used capacity or “lit capacity” is much less, and this gives cable operators the capability to gradually increase usage in response to rising customer demand or suddenly shift vast amounts of Internet traffic when other cables are broken or damaged (Brake, 2019, p.1). The complex submarine cable systems laid along the seabed have been the vital foundation of communications for decades, carrying more than 97% of global data traffic and allowing for an unbroken flow of information to cross the continents (Submarine Telecoms Forum, 2025, p. 106).

This chapter begins by exploring the critical role and inherent vulnerabilities of submarine cables in *Submarine Cables: Essential yet Vulnerable*, highlighting their significance as invaluable infrastructure and examining their vulnerabilities. *Submarine Cables under International Law* provides a systematic review of the international legal frameworks and applicable rules governing this essential infrastructure. *The Inadequacy of the Current International Law System in Protecting Submarine Cables* explores the inadequacy of current international law systems in protecting submarine cables.

Submarine Cables: Essential yet Vulnerable

An essential global system

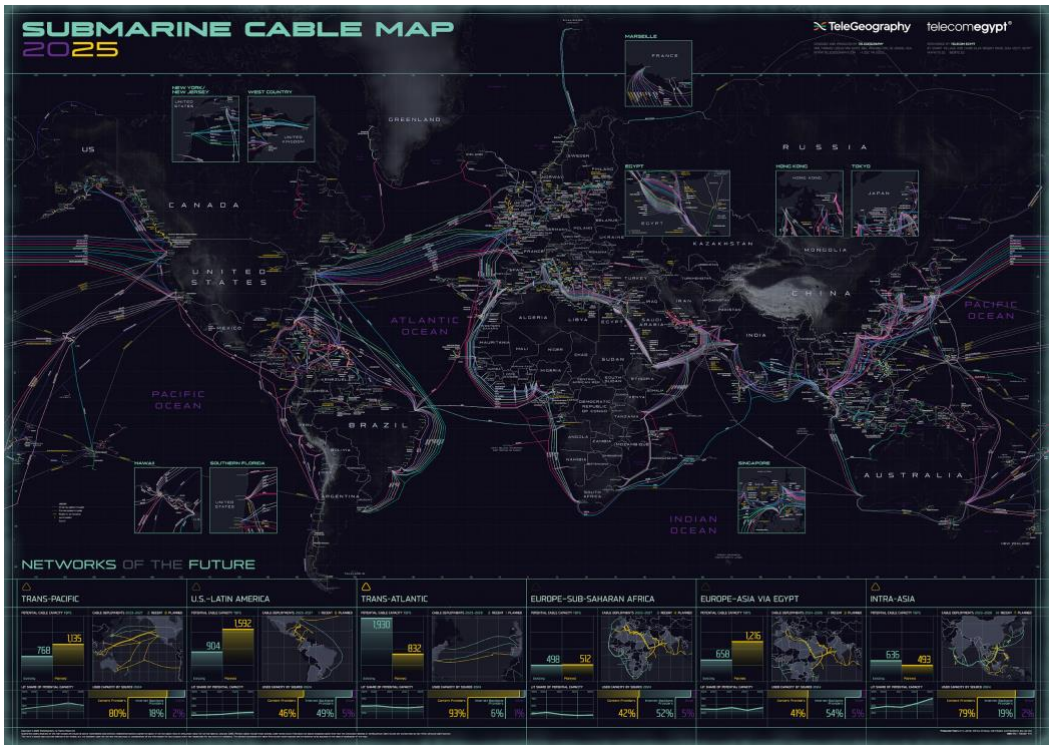
With the introduction of satellite communications technology in the 1970s and 1980s, a majority of global communications were transmitted via air rather than the outdated copper submarine cables that had been the primary means of transmission for over a century (Harbin, 2021. p. 355). The relatively low capacity of submarine cables meant that they were economically feasible only on the busiest routes during then (Carter et al, 2009, p. 15). However, the advent of fibre-optic technology in the late 1980s ultimately changed this dynamic.

In 1988, the first trans-oceanic fibre optic cable was installed, beginning a transformational change in the global communications infrastructure (Carter et al, 2009, p. 16). Fibre optics are much better suited for the increasing demand for high-speed and high-capacity communication links (Carter et al, 2009, p. 16). In contrast to satellite transmissions, which constantly suffer from latency due to their distance and are also significantly more expensive to deploy due to the complexity of space-based systems, fibre optic submarine cable systems offer huge bandwidths for a small fraction of the cost, creating an economic base from which the internet has been allowed to grow and evolve rapidly (Carter et al, 2009, p. 16). In essence, these fibre-optic cables made it possible to transmit enormous amounts of voice and data traffic with greater speed and security than ever before (Carter et al, 2009, p. 16). The internet infrastructure itself made that information not only accessible but also usable for a wide array of purposes, from communication to commerce, entertainment, education, and beyond (Carter et al, 2009, p. 16). It is not even in the same league as satellite technology in terms of volume, speed, and general cost-effectiveness (Carter et al, 2009, p. 16).

However, a common misconception in the modern era is that most international communications are transmitted through satellite systems, whereas, in fact, around 97% of international data traffic is actually routed through submarine fibre-optic cables, which form the

backbone of global connectivity infrastructure (Sunak, 2017, p. 2; Submarine Telecoms Forum, 2025, p. 106).

Figure 3.1: *The Global Submarine Cable Map in 2025*



Source: (TeleGeography, 2025)

The interconnected undersea network of submarine cables encompasses 597 active or under-construction cable systems and 1,712 landings, as shown in the map above (TeleGeography, 2025). Today, the vast majority of the world's communication is dependent on 1.4 million kilometres of active submarine cables that crisscross the planet, varying in length from several hundreds of kilometres (*such as spur cables*) to long-distance cables like the recently installed 2Africa cable that is an astonishing 45,000 kilometres long (Gervasi, 2023; Kentik, n.d.).

The International Network Volume of the Internet has expanded immensely. Inscribing an economical and consistent baseline, these cables have propelled the journey of connectivity—from the nascent days of the World Wide Web to the dynamic demands of today's hyper-scale customers (Submarine Telecoms Forum, 2025, p. 31). They are the foundation of modern life by transmitting data that powers everything from international banking and airline bookings to cat videos, socialisation, military communications, and the movement of goods around the world (Submarine Telecoms Forum, 2025, p. 31). This critical piece of global infrastructure, which we often take for granted, is under threat from a multitude of dangers and is far more exposed than many understand.

A vulnerable global system

The aggregation of high-capacity bandwidth circuit in a limited number of carrier hotels is a major weakness. Several hundred network operators interconnect their circuits in one nonsecure building. These buildings often feed directly into the international cable system where security is often 'farcical' (Fonow, 2006).

> "[I]f one or two of these facilities were even partly destroyed by attackers, a natural disaster or internal sabotage, cascading failures could immobilize much of the international telecommunication systems and Internet for several weeks. The effect on international finance, military logistics, medicine, commerce and agriculture in a global economy would be profound. A degraded system of military logistics would leave troops in the field with less support. The international flow of oil and food supplies would be impeded. Chaos in the shipping and airline industries would result. The system that supports e-mail, Word and Excel file transfers would be gone. Electronic funds transfers, credit card transactions and international bank reconciliations would slow to a crawl. […] [S]uch an event would cause a global depression" (Fonow, 2006)."

While submarine cables now provide the majority of long-distance international Internet and voice calls, this critical piece of infrastructure is not exempt from global vulnerabilities and is still a system that is susceptible to the effects of natural disasters and disruption from State and non-State actors (Sunak, 2017, p. 19). According to Submarine Telecoms Forum's data from the years 2015 to 2024: 237 publicly reported cable faults in various regions (Submarine Telecoms Forum, 2025, p. 86). The vast majority of them had human activity written all over them, almost always resulting in damage (Submarine Telecoms Forum, 2025, p. 86). Additionally, whereas natural disasters such as earthquakes and underwater volcanic eruptions have been a considerable factor in cable faults, such events have been less frequent (Submarine Telecoms Forum, 2025, p. 86). According to regional analysis, Austral-Asia was the most fault-prone region, with 36.3% of all reported faults. EMEA (Europe, Middle East and Africa) is second in contribution (28.7%) followed by Americas (20.3%) (Submarine Telecoms Forum, 2025, p. 86). The Indian Ocean, Transpacific, and Transatlantic regions all have reported similar low percentages, with less than 10% of all fault stories attributed to them (Submarine Telecoms Forum, 2025, p. 86).

The severing of submarine cables in the Luzon Strait in 2006 shows the way that natural disasters can block international connectivity. The Luzon Strait is a 160-mile stretch of open water between Taiwan and the northernmost island of the Philippines, and it is the only viable route (*the waters between China and Taiwan are too shallow*) for undersea cables to connect Hong Kong,

Taiwan, South Korea, and Japan (Sunak, 2017, p. 19). On 26 December 2006 at 8:26 pm, a huge earthquake struck the Luzon Strait, causing powerful undersea landslides that snapped six of the seven undersea cables used to transmit internet and phone services from North America to Taiwan, China, Hong Kong, Japan, Singapore, and South Korea (New Scientist, 2007; Sunak, 2017, p. 19).

The impact was immediate and severe. Chunghwa Telecom, Taiwan's largest telecom operator, reported a complete internet outage to Hong Kong and Southeast Asia, severing connectivity for millions of citizens and businesses (Qiu, 2006). In Seoul, trading of the Korean won halted abruptly, while in Hong Kong, 80% of communications capacity evaporated in just a few minutes—leaving Asia's critical financial hub dependent on one surviving cable to carry billions of dollars' worth of trades and transfers around the world (BBC News, 2006; Sahari, 2017). It would require 11 ships and nearly two months to patch the repairs, with the region's economic stability resting on a single fibre-optic cable no wider than a garden hose (Dzieza, 2024).

In addition to natural disasters, human activities present significant threats to the connectivity of global submarine cable networks. These cables are vulnerable to being cut, and the availability of maps detailing their exact locations only amplifies this risk (Sunak, 2017, p. 23). Most of these cables are positioned far from any detection or monitoring systems capable of tracking hostile maritime activity and damage occurring at such extreme depths is difficult to pinpoint and repair (Sunak, 2017, p. 23).

For example, in the spring of 2013, the Egyptian navy arrested three scuba divers off the coast of Alexandria, accusing them of attempting to cut the Southeast Asia Middle East Western Europe 4 [*SEA-ME-WE 4*] internet cable (BBC News, 2013). Spanning approximately 18,800 km and connecting Singapore, Malaysia, Thailand, Bangladesh, India, Sri Lanka, Pakistan, United Arab Emirates, Saudi Arabia, Egypt, Italy, Tunisia, Algeria and France, *SEA-ME-WE 4* carries heavy internet traffic between Europe and Egypt (Submarine Networks, n.d.). The severance of *SEA-ME-WE 4* would have caused significant disruption to global communications.

Significant challenges for the submarine cable networks also come from geopolitical tensions. For example, the Red Sea has become a hotspot for disruptions. Earlier in 2024, several underwater cables were reported damaged in the region, apparently by Houthi rebels, drastically disrupting internet traffic between Europe, Asia, and the Middle East (Submarine Telecoms Forum, 2025, p. 60). The outage affected up to 70% of data traffic along major routes (Submarine Telecoms Forum, 2025, p. 60).

A more complicated but subtle attack on the submarine cables would be tapping them and recording, copying or stealing data which can be later analysed for potential criminal activities (Wall

et al, 2021). This can be achieved by (i) embedding backdoors during the cable manufacturing process, (ii) targeting onshore landing stations and facilities linking the submarine cable to terrestrial networks, or (iii) tapping the cables at sea. (Wall et al, 2021).

Another potential type of attack would be cyber or network attacks where the network management systems which the private companies use to manage data traffic passing through the cables are hacked by malicious actors to disrupt data flows (Wall et al, 2021). Such malicious actors could gain control or administrative rights of a network management system when they would discover physical vulnerabilities or disrupt or divert data traffic or even execute a "kill click" deleting the wavelengths used to transmit data (Wall et al, 2021). For example, the recent SolarWinds and Colonial Pipeline cyberattacks also exposed the vulnerabilities of the US private sector with dramatic implications for national security (Wall et al, 2021).

A military capability

Subsea fiber-optic cables have the potential to be utilised as sensors which can help the naval defence intelligence, surveillance activities and serve as an early warning for countries from unwanted foreign operations through the use of Distributed Acoustic Sensing [DAS], a technique which relies on fiber optic to detect pressure waives from acoustics of seismic activity (Munro et al, 2023).

DAS requires using "dark" fiber (*i.e. an unused fiber in the cable*) (Munro et al, 2023) Light pulses are transmitted across the dark fiber through an interrogator (Munro et al, 2023). Any fluctuation in the reflected light which the interrogator senses can be translated by the advanced signal processing (Munro et al, 2023). This technology can cover greater distance by leveraging dark fibers in the existing commercial subsea cables (Munro et al, 2023). DAS has an incredible potential in subsea defence by providing the capability to track both surface and subsurface targets (Munro et al, 2023). Although the range is currently limited, the data can be effectively integrated into naval intelligence capabilities (Munro et al, 2023).

For example, in 2021, a study used a 41.5 km long cable off the coast of France to detect a vessel first 5.8 km offshore in 85m depth, and then 20 km offshore at 2,000m depth. Although the signal-to-noise ratio was better at the shallower depth, low frequency signal (*below 50 Hz*) was detected even at 2,000m (Agarwal, 2025). Research has further developed, and it now focuses on localisation of the vessel and classification (*i.e. identifying the type of the vessel*) (Agarwal, 2025). The legal framework discussed in *The Inadequacy of the Current International Law System in Protecting Submarine Cables* of this Chapter addresses the threats posed to submarine cables from the perspective of these cables being an effective means of communication. However, there

is no regulatory framework in place to address the recent development where DAS can be used as a military capability.

Submarine Cables under International Law

The submarine cables that connect people, places, and businesses are the lifeblood of the internet. The security, stability, and resilience of these cables are crucial to ensure the continued operation of global communications and commerce. International laws and conventions establish certain degrees of protection for these cables, but current legal mechanisms fall woefully short of responding to modern threats. A stronger and more adaptive legal regime is needed to protect this critical piece of infrastructure, as geopolitical tensions, cyber vulnerabilities, and technological advances will continue to grow.

1884 Convention for the Protection of Submarine Telegraph Cables

The first major international legal attempt to protect submarine cables came in the form of the 1884 Convention for the Protection of Submarine Telegraph Cables (*the "1884 Convention"*). In 1884, faced with the danger posed by fishermen and pirates, who inadvertently or sometimes still intentionally cut telegraph lines, 27 States gathered to draft the 1884 Convention for the Protection of Submarine Telegraph Cables (Wagner, 1995, p. 128). In 1882 and 1884, this Convention sprang from two summers of negotiations in Paris between delegates not just of diplomats, but also of fishermen, naval officers and electrical engineers (Burnett, 2021, p. 1671). Their collective goal was to craft a legal framework that addressed nearly two decades of global experience with the transformative technology of international submarine telegraph cables (Burnett, 2021, p. 1671). This treaty was intended to protect cables from deliberate or negligent damage that would disrupt the telegraph (Convention for the Protection of Submarine Telegraph Cables, 1884, Article II).

> "It is a punishable offence to break or injure a submarine cable, wilfully or by culpable negligence, in such manner as might interrupt or obstruct telegraphic communication, either wholly or partially, such punishment being without prejudice to any civil action for damages" (Convention for the Protection of Submarine Telegraph Cables, 1884, Article II).

The 1884 Convention sought to balance the interests of communication networks, maritime industries, and national security, laying the foundation for modern submarine cable protection under international law (Convention for the Protection of Submarine Telegraph Cables, 1884, Articles I - XVII). The 1884 Convention was created before the advent of modern internet-dependent submarine cables and certainly before modern cyber espionage threats, such as

hacking into such cables and intercepting sensitive data. Although at its conception, the Convention targeted physical damage to telegraph cables only, its provisions could, in theory, constitute a limited legal framework for certain types of submarine interference in contemporary situations.

According to Article II, the 1884 Convention applied to all legally established submarine cables outside territorial waters and made it an offence punishable by law for damages caused to submarine cables, whether intentional or due to culpable negligence. Unauthorised intrusion into submarine cables, whether through physical tampering or covert interception, inevitably causes some degree of damage and service disruption to access transmitted data. Any non-consensual entry point to submarine cables, including physical tampering or covert interception, can result in a net loss or degrading impact on the integrity of transmitted data. Such acts by State or non-state actors could, therefore, fall within the purview of Article II of the 1884 Convention, which makes wilful or negligent breaking or injury to submarine cables of great powers a punishable offence.

The 1884 Convention provides enforcement jurisdiction, which allows officers to "demand from the captain or master the production of the official documents proving the nationality of the said vessel, when the officers commanding the ships of war, or ships specially commissioned for the purpose by one of the High Contracting Parties, have reason to believe that an infraction of the measures provided for in the present Convention has been committed by a vessel other than a vessel of war" (Convention for the Protection of Submarine Telegraph Cables, 1884, Article X). Nevertheless, this provision has limited effectiveness, as it applies only to the States party to the 1884 Convention. The 1884 Convention also relies on the State's power of prosecutions for infractions provided against by Articles II, V and VI of the Convention (Convention for the Protection of Submarine Telegraph Cables, 1884, Article IX).

> "It is understood that the stipulations of the present Convention do not in any way restrict the freedom of action of belligerents" (Convention for the Protection of Submarine Telegraph Cables, 1884, Article XV).

The protection of submarine cables is not absolute and may be suspended during times of war. Submarine cables have been viewed as a legitimate target under international law, as reflected by Article XV of the 1884 Convention. However, the military and strategic significance of submarine cables today far exceeds that of a century ago, given their critical role in global communications, financial transactions, and defence operations. In the absence of an international agreement to the contrary, some views were raised that there is little reason to dispute that submarine cables remain legitimate military targets during armed conflicts (Liao, 2019, p. 482).

The 1884 Convention has only 44 participating States, falling far short of a universally accepted treaty. Certain States with significant influence over submarine cable infrastructure, including both their protection and potential disruption, are not parties to the 1884 Convention. Notably, the People's Republic of China remains outside the list of participating States, raising questions about the treaty's effectiveness in ensuring comprehensive global compliance. As a result, its practical application remains limited.

Instead of establishing a comprehensive international tribunal to adjudicate submarine cable disputes or enforce treaty obligations, the 1884 Convention merely required States to enact their own national regulations for cable protection (Convention for the Protection of Submarine Telegraph Cables, 1884, Articles V - XI). This decentralised approach has resulted in inconsistent enforcement and gaps in legal coverage, rendering submarine cables vulnerable to a host of threats. Many other States party to the Convention, including Canada, failed to pass domestic laws to give effect to its terms, which further weakened its effectiveness and uniform application (Petty, 2021, p. 271). Even when States did implement domestic laws to give effect to the Convention, the protections they provided were frequently piecemeal and weak. For instance, the United States responded to the 1884 Convention by passing the 1888 Submarine Cable Act (Petty, 2021, p. 271). However, the statute's enforcement has been largely ineffective, as its penalties are minimal. Civil fines are capped at $5,000, and the U.S. Coast Guard does not actively pursue violations (47 USC § 21). Notably, there is no recorded instance of a criminal charge being brought under the Act, further highlighting its limited deterrent effect (Wagner, 1995, p. 128).

Although the 1884 Convention has limited application to contemporary threats facing submarine cables, it remains a historic milestone in international law. As the first treaty dedicated explicitly to protecting submarine cables, it laid the groundwork for future legal frameworks governing undersea infrastructure. Its adoption marked a critical step in recognising the need for international cooperation in safeguarding global communications, setting a precedent for subsequent treaties and regulatory developments in maritime and telecommunication law.

1958 Convention on the High Seas and 1958 Convention on the Continental Shelf

The 1884 Convention represents the first international initiative aimed at regulating activities related to submarine cables. While its primary objective was to safeguard submarine telegraph cables from wilful or negligent damage, its influence extended beyond its original scope. Notably, the 1884 Convention's core provision on cable protection, articulated in Article II, was later incorporated into the 1958 Geneva Conventions on the High Seas and the 1958 Convention on Continental Shelf.

> "The high seas being open to all nations, no State may validly purport to subject any part of them to its sovereignty. Freedom of the high seas is exercised under the conditions laid down by these articles and by the other rules of international law. It comprises, inter alia, both for coastal and non-coastal States: […] (4) Freedom to lay submarine cables and pipelines; […] These freedoms, and others which are recognized by the general principles of international law, shall be exercised by all States with reasonable regard to the interests of other States in their exercise of the freedom of the high seas" (Convention on the High Seas, 1958, Article 2).

Article 2 of the 1958 Convention on the High Seas enshrined the freedom to lay submarine cables as one of the great high seas' freedoms, thereby extending significantly the legal framework that governs submarine cables. To reinforce this point, Article 26 of the 1958 Convention on the High Seas States, "States shall be entitled to lay submarine cables and pipelines on the bed of the high seas", creating an unequivocal legal basis for such activities (Convention on the High Seas, 1958, Article 26). By explicitly recognising and securing the freedom to lay submarine cables as a core principle of maritime law, the 1958 High Seas Convention laid the foundation for modern treaty obligations concerning undersea infrastructure.

The 1958 Convention on the High Seas represented a significant milestone in the international community's recognition of the vital role submarine cables play in global communications and commerce. However, it also made clear that the freedom to lay submarine cables was not absolute. States exercising this right were required to do so with due regard for the interests of other States, particularly in relation to activities such as fishing and navigation, which could potentially interfere with cable operations (Convention on the High Seas, 1958, Articles 2 & 26). By introducing this obligation, the 1958 Convention on the High Seas sought to balance the expansion of submarine cable networks with the broader maritime interests of coastal and high seas users.

> "Subject to its right to take reasonable measures for the exploration of the continental shelf and the exploitation of its natural resources, the coastal State may not impede the laying or maintenance of submarine cables or pipelines on the continental shelf" (Convention on the High Seas, 1958, Article 4).

The 1958 Convention on the Continental Shelf, for example, explicitly recognises the freedom to lay submarine cables, just as Article 4 of the Convention provides that this freedom must be exercised subject to the coastal State's right to take the necessary measures for exploration and exploitation of its natural resources.

Although this provision recognises the interests of submarine cable protections versus coastal State sovereignty, the 1958 Convention on the Continental Shelf is vague about how to draw the line between these conflicting interests. The generic formulation in the absence of specific guidelines creates an opportunity for uncertainty, which might trigger disputes over coastal State jurisdiction vis-à-vis other States' rights to lay and maintain submarine cables.

1982 United Nations Convention on the Law of the Sea [UNCLOS]

Recognising the developments since the 1958 and 1960 United Nations Conferences on the Law of the Sea, the UNCLOS underscores the necessity of establishing a new, broadly accepted international agreement to address contemporary maritime challenges (UNCLOS, 1994, Preamble). UNCLOS affirmed the role of unilateral State action in shaping customary international law to align with evolving realities and technological advancements (Harbin, 2021, p. 376). It establishes a comprehensive international legal framework for the world's seas. UNCLOS also recognises the interrelated nature of ocean problems, noting that they should not be addressed in isolation but rather as part of a comprehensive approach that takes into account the interactions between navigation, resource management, environmental conservation, and national jurisdiction (UNCLOS, 1994, Preamble).

UNCLOS established a foundational framework for the development and regulation of submarine infrastructures. The preamble reinforces the principles of United Nations General Assembly Resolution 2749 (XXV) of 1970, which declared that the seabed, ocean floor, and its subsoil beyond national jurisdiction—along with their resources—are the common heritage of mankind. It affirms that the exploration and exploitation of these areas should benefit all humanity, regardless of a State's geographical position (UNCLOS, 1994, Preamble; United Nations General Assembly Resolution 2749, 1970, XXV). Compared to the 1958 Convention on the High Seas and the 1958 Convention on the Continental Shelf, UNCLOS functions as a more comprehensive legal instrument for addressing international law issues related to submarine cables.

Rights and obligations for States regarding submarine cables

> "The high seas are open to all States, whether coastal or land-locked. Freedom of the high seas is exercised under the conditions laid down by this Convention and by other rules of international law. It comprises, inter alia, both for coastal and land-locked States: […] freedom to lay submarine cables and pipelines, subject to Part VI; […]" (UNCLOS, 1994, Article 87)

> "All States are entitled to lay submarine cables and pipelines on the bed of the high seas beyond the continental shelf. […]" (UNCLOS, 1994, Article 112)

UNCLOS inherited the fundamental principle that the high seas are open to all States, regardless of whether they have a coastline or are landlocked, which ensures that landlocked States are not disadvantaged and can still participate in the laying of submarine cables for communication and economic purposes.

UNCLOS recognises States' regulatory power to enact laws and regulations for the protection of submarine cables in their territorial sea. States are entitled to regulate innocent passage by foreign vessels to ensure that submarine cables and pipelines falling under their jurisdiction are not damaged or disrupted (UNCLOS, 1994, Article 21). However, this right is not absolute—it must be exercised in conformity with UNCLOS and other international legal norms to prevent excessive restrictions on navigation rights (UNCLOS, 1994, Article 51).

The UNCLOS implicitly recognises that archipelagic States have jurisdiction over their archipelagic waters, meaning that foreign States cannot freely undertake maintenance activities without informing the host State (UNCLOS, 1994, Article 51). Archipelagic States retain the right to be notified of any repair or replacement operations in their waters. This allows them to ensure such activities align with their domestic regulations and environmental policies (UNCLOS, 1994, Article 51). Archipelagic States are entitled to some notice of repair or replacement activities in their waters (UNCLOS, 1994, Article 51). This enables them to verify that such operations adhere to their national rules and environmental regulations.

In addition, archipelagic States must recognise and respect submarine cables that were previously laid by other States before the waters were designated as archipelagic waters, ensuring these cables remain undisturbed (UNCLOS, 1994, Article 51). In case of maintenance, archipelagic States have the obligation to permit the maintenance and replacement of these cables, provided they receive prior notice of the location and intended work (UNCLOS, 1994, Article 51). This obligation prevents archipelagic States from unreasonably obstructing essential communication and data transmission networks. UNCLOS thus prevents States from abusing their sovereignty to restrict foreign submarine cables arbitrarily.

Table 3.1: *Comparing Aspects of UNCLOS Articles*

Aspect	Article 58 of UNCLOS (EEZ)	Article 79 of UNCLOS (continental shelf)

Who has rights to lay submarine cables?	All States (coastal and landlocked)	All States (coastal and landlocked)
Can Coastal States interfere?	No, unless justified under UNCLOS	No, but they may regulate routes and environmental concerns
Obligations of States laying cables	Must comply with UNCLOS and respect coastal State rights	Must avoid damaging existing cables, comply with coastal State regulations

Article 58 of UNCLOS regulates State's rights and obligations in the Exclusive Economic Zone [EEZ]. This Article grants all States—both coastal and landlocked—the right to lay submarine cables and pipelines in the EEZ (UNCLOS, 1994, Article 58). This means that States do not need coastal State permission to lay cables in the EEZ, as long as they comply with the relevant provisions of UNCLOS. Meanwhile, coastal States cannot be unreasonable in prohibiting other States from running cables through their EEZ. The rights granted by this clause are not unlimited—States must engage in activities that are consistent with other aspects of UNCLOS, such as refraining from activities that could be harmful to the marine environment or interfere with other lawful activities taking place within the EEZ (UNCLOS, 1994, Article 58).

Article 79 of UNCLOS regulates State's rights and obligations on the continental shelf. All States, including landlocked States, have the right to lay submarine cables and pipelines on the continental shelf, provided they follow the provisions of UNCLOS (UNCLOS, 1994, Article 79). Coastal States cannot arbitrarily prevent or interfere with the laying or the maintenance of submarine cables and pipelines (UNCLOS, 1994, Article 79). States that laying submarine cables have the right to repair and maintain them, and when laying new submarine cables, State must respect pre-existing infrastructure and ensure that repair access to older cables is not obstructed (UNCLOS, 1994, Article 79).

UNCLOS provides that coastal States can take reasonable measures to protect their continental shelf resources, marine environment, and pollution control efforts, which means that States laying submarine cables must not interfere with activities like offshore oil drilling or marine conservation zones (UNCLOS, 1994, Article 79). The jurisdiction of coastal states extends to cables connecting artificial islands, installations, or other resource-extraction facilities under its control (UNCLOS, 1994, Article 79).

Liabilities for damaging submarine cables

> "Every State shall adopt the laws and regulations necessary to provide that the breaking or injury by a ship flying its flag or by a person subject to its jurisdiction of a submarine cable beneath the high seas done wilfully or through culpable negligence, in such a manner as to be liable to interrupt or obstruct telegraphic or telephonic communications, and similarly the breaking or injury of a submarine pipeline or high-voltage power cable, shall be a punishable offence. […]" (UNCLOS, 1994, Article 113).

The UNCLOS requires the State to regulate and enforce laws on ships flying its flag that damage submarine cables on the high seas. If a ship damages a submarine cable, the flag State has the jurisdiction to investigate and prosecute the responsible parties (UNCLOS, 1994, Article 113). The clause recognises an exception for ships acting in distress. That is, if a vessel damages a cable while legitimately trying to save lives or its own safety, it cannot be held criminally liable.

By textual interpretation of Article 113 of UNCLOS, States have the obligation to enact national laws making it a punishable offense to intentionally or negligently break or damage a submarine cable, which is a proactive duty on States to regulate risky maritime activities that could endanger undersea infrastructure.

> "Every State shall adopt the laws and regulations necessary to provide that, if persons subject to its jurisdiction who are the owners of a submarine cable or pipeline beneath the high seas, in laying or repairing that cable or pipeline, cause a break in or injury to another cable or pipeline, they shall bear the cost of the repairs" (UNCLOS, 1994, Article 114).

Under Article 114, UNCLOS requires States to establish domestic legal frameworks to ensure that cable and pipeline owners are held financially responsible for any damage they cause to existing infrastructure.

> "Every State shall adopt the laws and regulations necessary to ensure that the owners of ships who can prove that they have sacrificed an anchor, a net or any other fishing gear, in order to avoid injuring a submarine cable or pipeline, shall be indemnified by the owner of the cable or pipeline, provided that the owner of the ship has taken all reasonable precautionary measures beforehand" (UNCLOS, 1994, Article 115).

Article 115 of UNCLOS obliges States to enact domestic legislation by which such owners of ships are entitled to indemnification for losses sustained in preventing damage to the cable. For

example, the submarine cable owner will be liable to compensate the ship owner for the pre-emptive sacrifice of such equipment (such as a ship's anchor or fishing gear) to protect the cable from damage. This Article of UNCLOS encourages relevant parties to protect submarine cables and protects fishermen and maritime operators who act responsibly to protect undersea infrastructure. Such compensation is only granted if the ship owner has taken all reasonable precautions beforehand, which ensures that ship owners act responsibly and do not engage in reckless conduct that might risk damaging submarine cables.

The Inadequacy of the Current International Law System in Protecting Submarine Cables

Submarine cable installation and repair, including the laying, operation, and maintenance of submarine cables, as well as the construction of submarine cable systems, are predominantly conducted by private entities rather than governments (Brendon & Bhatt, 2024). This private-sector dominance has contributed to a lack of direct communication and cooperation between the submarine cable industry and coastal States. Consequently, many coastal States have little incentive to protect submarine cables that land in their territory actively, even though they have now been extensively recognised as international "public goods" that serve critical issues in global communications (Liao, 2019, p. 459). Moreover, there also remains a troubling lack of government awareness of the strategic significance of submarine cables (Liao, 2019, p. 459). This can be attributed, in part, to the widespread misconception that the majority of international communications are transmitted via satellites rather than through undersea cable networks (Liao, 2019, p. 459). Additionally, the success and effectiveness of the submarine cable industry in maintaining and repairing its own infrastructure with little government intervention may have bred complacency among policymakers, further diminishing the perceived need for them to prioritise the protection and regulation of submarine cables (Liao, 2019, p. 459).

Although the 1884 Convention for the Protection of Submarine Telegraph Cables, the 1958 Convention on the High Seas, the 1958 Convention on the Continental Shelf and the 1982 United Nations Convention on the Law of the Sea provide a basic framework for protecting submarine cables, such protection is inadequate.

For example, Article 58 of UNCLOS, which governs the rights and duties of States in the EEZ, extends the applicability of Articles 88 to 115 of UNCLOS to the EEZ, provided they are not inconsistent with other part of UNCLOS (UNCLOS, 1994, Article 58). Article 113 of UNCLOS imposes an obligation on all States to enact national legislation that criminalises the wilful or culpably negligent breaking or injury of submarine cables beneath the high seas when such actions interfere with telegraphic or telephonic communications (UNCLOS, 1994, Article 113). This

provision is grounded in both national jurisdiction and flag State jurisdiction (UNCLOS, 1994, Article 113). However, these provisions under UNCLOS do not provide sufficient protection for submarine cables against intentional acts of damage, including those arising from terrorism or sabotage. One fundamental limitation is that Articles 113 and 58(2) confer only prescriptive jurisdiction upon States, meaning they establish an obligation to criminalise such offences through national legislation, but they do not grant enforcement jurisdiction to act against violations in real-time (Liao, 2019, p. 460).

Enforcement of these provisions remains constrained by the principle of exclusive flag State jurisdiction, which dictates that only the State under whose flag a vessel is registered has the authority to take enforcement action against that vessel on the high seas (National Oceanic and Atmospheric Administration, n.d.). This principle, aimed at preventing undue interference by other States, effectively limits the ability of coastal or third-party States to intervene against vessels suspected of engaging in acts of cable sabotage, even when those acts pose a serious threat to global communications and security (Liao, 2019, p. 460). Furthermore, the effectiveness of Article 113 of UNCLOS is largely undermined by the fact that most States have not incorporated it into their domestic legal frameworks. In practice, this means that the deliberate breaking or damaging of submarine cables on the high seas or within the EEZ of coastal States is not classified as a criminal offence in the national laws of many States (Liao, 2019, p. 460). Except in the few cases where States have adopted national legislation compliant with Article 113, the penalties have often proved to be not sufficiently severe so as to act as an effective deterrent to deliberate damage to submarine cables (Convention for the Protection of Submarine Telegraph Cables, 1884, Article III, Subsection A). Therefore, despite the provisions of UNCLOS, the weak implementation and enforcement of Article 113 contribute to the continued susceptibility of submarine cables to intentional disruption.

Articles 58 and 113 of UNCLOS stand in contrast to Article X of the 1884 Convention, which grants warships the authority to demand documentation from a vessel's captain or master as proof of its nationality when there are allegations of submarine cable damage (Convention for the Protection of Submarine Telegraph Cables, 1884, Article X). Article X of the 1884 Convention theoretically establishes enforcement jurisdiction to audit and authenticate vessels suspected of malfeasance with respect to cables, thus enabling potential accountability. However, there are still limitations to the practical effect of Article X of the 1884 Convention. First, the provision only applies to States that are parties to the 1884 Convention, severely limiting its jurisdictional reach in contemporary maritime governance. Secondly, even among those parties, the provision is rarely invoked, further diminishing its utility as a deterrent or enforcement mechanism (Liao, 2019, p.

460). As a result, the 1884 Convention's narrow applicability and infrequent use render it largely ineffective in contemporary submarine cable protection efforts.

Beyond Articles 58 and 113, a competitive dynamic exists between the activities undertaken by coastal States—such as fisheries, the exploration and exploitation of continental shelf resources, and the establishment of artificial islands—and the rights of foreign nationals to lay and operate submarine cables (Liao, 2019, p. 462). This tension arises because, under UNCLOS, the laying and maintenance of submarine cables in the continental shelf and EEZ are recognised as rights of foreign States' nationals, deriving from the freedom of the high seas rather than being subject to coastal State control (UNCLOS, 1994, Article 58 & 79). This contrast is explicitly articulated in Article 79(2) of UNCLOS, which provides that, while a coastal State has the right to take reasonable measures for the exploration of the continental shelf, the exploitation of its natural resources, and pollution control from pipelines, it may not impede the laying or maintenance of submarine cables or pipelines (UNCLOS, 1994, Article 79). This provision reflects a balance between coastal State sovereignty over its resources and the freedom of all States to install and maintain submarine cables in the EEZ and continental shelf (UNCLOS, 1994, Article 79). However, potential conflicts arise as UNCLOS mandates that both coastal States and other States exercise their respective rights with "due regard" for one another's interests in the EEZ (UNCLOS, 1994, Articles 57 & 58). In certain cases, these regulatory measures may arguably extend beyond what is permissible under UNCLOS, leading to disputes over the lawful extent of coastal State authority in regulating submarine cable infrastructure (Liao, 2019, p. 462).

For example, a key issue in the regulation of submarine cables concerns the freedom to conduct repair and maintenance operations. It is arguable that submarine cable repair falls within the scope of Article 58(1) of UNCLOS, which recognises "other internationally lawful uses of the sea" related to submarine cables, provided such activities are compatible with other provisions of UNCLOS (Liao, 2019, p. 463). This interpretation suggests that the repair of submarine cables should be considered a lawful activity under the general freedoms associated with submarine cables in the EEZ. State practice on this matter, however, varies significantly. A number of States—including Australia, Japan, and several European nations—do not require permits for emergency submarine cable repairs, even within their territorial sea, thereby facilitating swift restoration of communication infrastructure (Liao, 2019, p. 463). Conversely, some States, such as China and India, impose permit requirements for cable repairs in their EEZs, adding a regulatory layer that may delay urgent maintenance work and hinder the timely restoration of communication services (Liao, 2019, p. 463).

Despite its comprehensive framework for maritime governance, UNCLOS leaves some critical issues unresolved, particularly regarding threats such as terrorism targeting submarine cables. A hypothetical but plausible scenario highlights this jurisdictional gap: suppose terrorists—who are nationals of State A—use a ship registered in State B to deliberately destroy submarine cables located in the EEZ of State C, with the intent of disrupting State C's internet and communication infrastructure (Liao, 2019, p. 464). Under Article 113 of UNCLOS, responsibility for prosecuting such acts primarily falls on State A and State B, provided they have enacted domestic legislation criminalising the wilful or negligent destruction of submarine cables (Liao, 2019, p. 464). However, the jurisdictional authority of State C—the State suffering direct harm from the attack—is far less clear under UNCLOS, as the destruction occurs outside its territorial waters (Liao, 2019, p. 464). This ambiguity poses significant challenges in cases where States A and B have not implemented Article 113 in their domestic laws, meaning that the perpetrators may not face prosecution at all. Even if such laws exist, jurisdictional enforcement gaps arise when States A and B are either unwilling or unable to prosecute offenders. As a result, State C may lack a clear legal basis under UNCLOS to assert jurisdiction despite being the primary victim of the attack. This limitation in UNCLOS's jurisdictional framework thus raises concerns about the effectiveness of existing international legal mechanisms in addressing transnational threats to critical submarine cable infrastructure.

The inadequacy of both international and domestic law in ensuring the protection of submarine cables arises from the longstanding tension between coastal State interests and the high seas freedoms associated with submarine cable operations (Liao, 2019, p. 464). Under the current legal framework, coastal States lack a clear jurisdictional basis to criminalise intentional damage to submarine cables occurring in maritime areas beyond their territorial sea, despite the fact that such acts may have severe economic and security implications for them (Liao, 2019, p. 465). This jurisdictional gap is particularly problematic in cases of terrorist attacks or deliberate sabotage, as coastal States—while being the primary victims of such acts—are legally constrained in their ability to prosecute offenders when the destruction occurs in the EEZ or on the continental shelf (Liao, 2019, p. 465). This limitation appears counterintuitive, given that it is often the coastal States that bear the consequences of these attacks, including disruption of communications, financial transactions, and critical infrastructure services (Liao, 2019, p. 465). While some coastal States have responded by establishing submarine cable protection zones, these regulatory efforts reflect a growing recognition of the strategic importance of submarine cables (Liao, 2019, p. 465). However, the legal authority to prescribe and enforce such protection zones under UNCLOS remains ambiguous, leaving many issues unresolved under international law.

Conclusion

Since the installation of the first commercial submarine cable across the English Channel in the 1850s, submarine cables have profoundly transformed global communication, drastically reduced transmission delays and laid the foundation for modern telecommunications. Today, approximately 1.4 million kilometres of active submarine cables underpin global connectivity (Kentik, n.d.)

Submarine cables constitute the backbone of the global communications infrastructure, transmitting over the majority of international data and enabling the transcontinental flow of information. In addition to their commercial and civilian utility, these systems are increasingly regarded as strategic military assets, particularly in light of dual-use capabilities facilitated by DSA technologies. However, submarine cable systems remain acutely vulnerable. They are exposed to a broad spectrum of threats, both natural and human-induced, which are frequently underestimated in legal, regulatory, and policy frameworks. These vulnerabilities encompass environmental hazards such as seismic events and other natural disasters, as well as deliberate acts of disruption by both State and non-State actors. Recent instances of such interference include damage reportedly caused by armed groups such as the Houthi rebels, highlighting the susceptibility of these infrastructures to geopolitical instability and asymmetric threats.

While various international legal frameworks—including the 1884 Convention for the Protection of Submarine Telegraph Cables, the 1958 Conventions on the High Seas and the Continental Shelf, and the United Nations Convention on the Law of the Sea—govern their protection, these instruments are inadequate in addressing contemporary risks. Enforcement of the provisions of UNCLOS remains constrained by the principle of exclusive flag State jurisdiction. Article 58 and 113 of UNCLOS can be contrasted to Article X of the 1884 convention, which grants warships the authority to demand documentation from a vessel's captain or master as proof of its nationality when there are allegations of submarine cable damage. Nevertheless, practical difficulties, such as lack of communication between submarine cable industry and coastal States remain who have little incentive to protect submarine cables which land in their territory. Hence, significant legal challenges still persist in strengthening defence mechanisms against emerging threats to submarine cable infrastructure.

References

Agarwal S, (2025, March 3). *Underwater Domain Awareness for and by Submarine Communication Cables*. National Maritime Foundation. https://maritimeindia.org/underwater-domain-awareness-for-and-by-submarine-communication-cables/#_ftn37

Brake, D. (2019, April 19). *Submarine cables: Critical infrastructure for global communications*. Information Technology and Innovation Foundation. https://itif.org/publications/2019/04/19/submarine-cables-critical-infrastructure-global-communications/

BBC News. (2006, December 27). *Asia communications hit by quake*. https://cdnedge.bbc.co.uk/1/hi/world/asia-pacific/6211451.stm

BBC News. (2013, March 28). *Internet disrupted in Middle East after seawater cable cut*. https://www.bbc.co.uk/news/world-middle-east-21963100

Burnett, D. R. (2021). Submarine cable security and international law. *International Law Studies Series, U.S. Naval War College, 97*, 1659–1682.

Cannon, B. J., & Bhatt, P. (2024, February 8). *Policy recommendations for Quad cooperation on submarine cable protection in the Indo-Pacific*. Pacific Forum. https://pacforum.org/publications/pacnet-8-policy-recommendations-for-quad-cooperation-on-submarine-cable-protection-in-the-indo-pacific/

Carter, L., Burnett, D. R., Drew, S., Marle, G., Hagadorn, L., Bartlett-McNeil, D., & Irvine, N. (2009). *Submarine cables and the oceans: Connecting the world* (UNEP-WCMC Biodiversity Series No. 31). ICPC/UNEP/UNEP-WCMC.

Convention for the Protection of Submarine Telegraph Cables, March 14, 1884, entered into force May 1, 1888.

Convention on the High Seas, April 29, 1958, entered into force September 30, 1962.

Dzieza, J. (2024, April 16). *The invisible seafaring industry that keeps the internet afloat*. The Verge. https://www.theverge.com/c/24070570/internet-cables-undersea-deep-repair-ships

Fonow, R. (2006). *Cybersecurity demands physical security*. Armed Forces Communications & Electronics Association (AFCEA). https://www.afcea.org/signal-media/cybersecurity-demands-physical-security

Harbin, D. E., III. (2021). Targeting submarine cables: New approaches to the law of armed conflict in modern warfare. *Military Law Review, 229*(3), 349–380.

Kentik. (n.d.). *Diving deep into submarine cables: Undersea lifelines of internet connectivity*. https://www.kentik.com/blog/diving-deep-into-submarine-cables-undersea-lifelines-of-internet-connectivity/

Liao, X. (2019). Protection of submarine cables against acts of terrorism. *Ocean Yearbook, 33*.

Munro, B, and MacGillivray, I. (2023, September 29), *Reconsider Using Undersea Cables as Military Sensors,* National Defense, https://www.nationaldefensemagazine.org/articles/2023/9/29/reconsider-using-undersea-cables-as-military-sensors

National Oceanic and Atmospheric Administration (NOAA). (n.d.). *Jurisdiction over vessels*. https://www.noaa.gov/jurisdiction-over-vessels

New Scientist. (2007, January 6). Earthquake shakes the internet. *New Scientist*. https://www.newscientist.com/article/mg19325852-300-earthquake-shakes-the-internet/

Petty, J. (2021). How hackers of submarine cables may be held liable under the law of the sea. *Chicago Journal of International Law, 22*(1), 260–298.

Sahari, S. (2017, June 14). *The root of a robust internet*. APNIC Blog. https://blog.apnic.net/2017/06/14/root-robust-internet/

Submarine Networks. (n.d.). *SEA-ME-WE 4*. https://www.submarinenetworks.com/en/systems/asia-europe-africa/smw4

Submarine Telecoms Forum, Inc. (2024). *Submarine telecoms industry report 2024 | 2025* (Issue 13). Submarine Telecoms Forum, Inc.

Sunak, R. (2017). *Undersea cables: Indispensable, insecure* (p. 12). Policy Exchange.

TeleGeography. (2025). *Submarine cable map 2025*. https://submarine-cable-map-2025.telegeography.com/

United Nations Convention on the Law of the Sea, December 10, 1982, entered into force November 16, 1994.

Wagner, E. (1995). Submarine cables and protections provided by the law of the sea. *Marine Policy, 19*(2), 127–136.

Wall, C and Morcos, P. (2021, June 11), *Invisible and Vital: Undersea Cables and Transatlantic Security,* Centre for Strategic and International Studies. https://www.csis.org/analysis/invisible-and-vital-undersea-cables-and-transatlantic-security

Submarine Networks. (2006). *Cables cut after Taiwan earthquake 2006*. https://www.submarinenetworks.com/en/nv/news/cables-cut-after-taiwan-earthquake-2006

1958 Convention on the Continental Shelf, April 29, 1958, entered into force June 10, 1964.

Chapter 4: Robustness of Tactical and Military Networks Against Natural Disasters and Hostile Environments: A Comprehensive Analysis of Military Communication Systems Resilience

Dr. Abdellah Chehri, ORCID: https://orcid.org/0000-0002-4193-6062
Dr. hab. Dorota Domalewska, ORCID: https://orcid.org/0000-0002-1788-1591

Abstract:
Military communication networks serve as the backbone of operational command and control, intelligence gathering, force coordination, and natural disaster management. This work provides a comprehensive analysis of military network resilience, emphasizing key strategies and challenges in the face of natural disasters and hostile disruptions. More precisely, it explores some components such as the choice of network architecture, redundancy mechanisms, encryption methodologies, physical security enhancements, and strategies for rapid deployment. By examining examples from recent military actions and disaster responses, the study shows how effective layered defense strategies, flexible routing methods, distributed network designs, and cross-domain solutions help maintain mission continuity under adverse situations. It also looks at how natural disasters like hurricanes, earthquakes, and cyberattacks affect communication reliability, and therefore reviews measures to reduce these risks to sustain operational functionality. The chapter concludes by presenting a forward-looking roadmap for research and development, identifying emerging threats and technological advancements that will shape next-generation military network resilience in complex battlespace environments.

Keywords: Communication, Resilience, Disaster Preparedness

Introduction

Military networks are the cornerstone of modern defense infrastructure, integrating communications, command and control [C2] systems, and intelligence, surveillance, and reconnaissance [ISR] capabilities. Due to their significance in critical infrastructure and national security, their resilience is essential for maintaining operating efficiency and achieving mission success. As threats evolve—such as cyberattacks, communication signal interference, and environmental challenges caused by climate change—these networks must be developed to withstand various forms of disruption (Cha et al., 2018; Chen et al., 2018; Middlebrooks et al., 2022; Suomalainen et al., 2021).

This study offers an in-depth examination of military network resilience, including the challenges, technological developments, architectural factors, and strategic frameworks essential

for improving operational resilience. The study also examines emerging technologies such as software-defined networking [SDN], automated network adjustments, quantum encryption techniques, and AI-driven strategies for threat mitigation (Suomalainen et al., 2021).

The originality of this study lies in its synthesis of established concepts, such as SDN and RF systems, with a holistic integration of disaster response mechanisms, emerging technologies (*e.g., AI and blockchain*), and recent case studies (*2023–2025*). In contrast to narrowly focused technical research, this paper offers an interdisciplinary analysis that brings together space-terrestrial network architectures, multi-domain operational contexts, and resilience strategies applicable to both combat and disaster scenarios. It contributes to current discussions on national and global security priorities, such as climate resilience, cyber warfare preparedness, and the protection of critical infrastructure, by proposing practical frameworks for disaster response and robust network design.

Threat Landscape: Challenges to Military Network Resilience

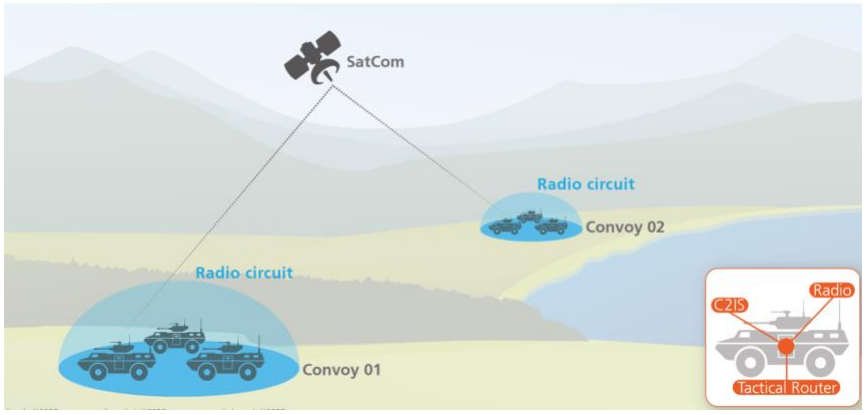
Military networks operate within an increasingly complex and adversarial threat landscape, where natural hazards and deliberate hostile actions pose significant risks to operational continuity. Ensuring the resilience of these networks requires a deep understanding of the diverse challenges that can compromise connectivity, data integrity, and command and control [C2] effectiveness.

Efficient resource utilization is critical when deploying Command and Control Information Systems [C2IS] in Disconnected, Intermittent, and Limited [DIL] networks. These environments demand optimized communication strategies to ensure operational effectiveness despite constraints in bandwidth, latency, and connectivity (Möhlenhof et al., 2021; Miao et al., 2022; Eswaran et al., 2012; Alquwayzani & Albuali, 2024; Jeon & Baek, 2024). To address these challenges, C2IS services need to be built with the ability to adapt and be aware of the network, so they can change based on the current connectivity situation. These goals can be achieved by sharing information between C2IS applications and tactical radio networks, along with smart resource management. These rules help the system respond effectively to changing network conditions. Such adaptive strategies allow for real-time assessment of available communication resources, making it easier to distribute them effectively among different nodes and services while also helping to avoid overwhelming the network (Waseem & Rana, 2025).

To illustrate the practical significance of specific cross-layer adaptations, one may analyze certain operational issues faced in military deployments. A typical situation involves a commander supervising two platoons, each equipped with tactical routers, battle radios, and C2IS systems. In individual platoons, low-data-rate Very High Frequency [VHF] radios function as the principal

communication channels. On the other side, the commander could employ a high-latency satellite communication [SATCOM] link for inter-platoon coordination (*which is shown in Figure 1*). The diverse network configurations emphasize the imperative for resilient and flexible command and control information systems [C2IS] capable of situational monitoring and ensuring mission continuity despite unpredictable situations.

Figure 4.1: *Hierarchical Tactical Communication Architecture for Platoon-Level Operations.*



Source: Suomalainen, J., Julku, J., Vehkaperä, M., & Posti, H. (2021). *Securing public safety communications on commercial and tactical 5G networks: A survey and future research directions*. *IEEE Open Journal of the Communications Society, 2*, 1590–1615. Licensed under Creative Commons Attribution 4.0 International (CC BY 4.0). © 2021 The Authors.

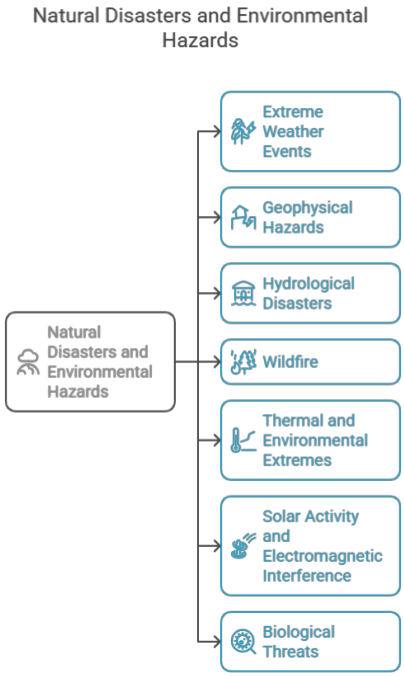
Natural Disasters and Environmental Hazards

Military communication infrastructures are inherently exposed to extreme environmental conditions that pose significant risks to operational effectiveness, system integrity, and long-term resilience. These problems can cause physical damage to important network parts, lead to power outages that disrupt communication, weaken signals due to weather and electromagnetic interference, and create difficulties in maintaining and restoring systems. Harsh weather and natural events can greatly disrupt military communication, so strong plans are needed to keep the network working well in difficult situations.

Natural catastrophes provide substantial threats to military communication networks, necessitating effective mitigation techniques. Inclement weather, seismic activity, and blizzards may jeopardize infrastructure and thus impair operations. Flooding can impede communication networks, while wildfires and excessive temperatures can compromise electrical facilities. Solar storms and electromagnetic pulses threaten unprotected systems, and satellite communication, while pandemics reduce workforce availability, obstructing maintenance and network restoration.

Strategic resilience planning is essential for ensuring operational continuity. Figure 2 provides an overview of natural disasters that may affect communication systems.

Figure 4.2: *Impact and Risk Assessment of Natural Disasters and Environmental Hazards.*



Hostile Actions and Intentional Disruptions

Military communication and control systems encounter increasingly complex threats that encompass cyber, electronic, and physical domains (Alkhamees & Milstein, 2024). Cyberattacks, spanning advanced persistent threats [APTs], malware, ransomware, and supply chain vulnerabilities, enable illegal access, loss of information, and severe operational disruptions. Electronic warfare strategies, including jamming, spoofing, and radio frequency interference, compromise network authentication and geolocation precision, affecting situational awareness in combat situations. Electromagnetic pulse [EMP] attacks pose a significant risk to unshielded systems, potentially causing catastrophic failures in military computing and communication architectures.

Directed energy weapons, including high-energy lasers and microwave disruptors, threaten communication networks and essential electronic components, impairing tactical connectivity. Mitigating these threats requires advanced defensive measures, resilient system architectures, and proactive threat detection strategies.

Mitigation and Strategic Considerations

Defending military networks against these diverse threats requires an integrated approach that combines redundancy planning, encryption protocols, reinforced infrastructure, software-defined networking, and adaptive networking technologies. Using methods like multi-layer encryption, artificial intelligence [AI]-based detection of unusual activity, changing frequencies, and software-defined networking for adjusting the network is crucial for improving the survival of military networks in challenging and damaged situations.

Software-Defined Networking in Tactical Networks

The development of military communication networks shows a constant interaction between the needs of operations and new technology, which influences the systems that support today's defense abilities. As battlefield environments grow more complex—driven by rapid force mobility, electronic warfare threats, and the demand for real-time intelligence—traditional network architectures struggle to adapt. The integration of software-defined networking [SDN] into tactical military environments represents a paradigm shift aimed at enhancing flexibility, resilience, and efficiency in mission-critical operations.

Evolution of Military Communications and the Need for SDN

Early military communications (*1940s–1960s*) mostly relied on analog radio systems with static infrastructure, constrained by manual routing and rigid command structures lacking agility. The implementation of digital technologies during the Cold War improved efficiency but remained centralized and vulnerable to disruptions. The establishment of ARPANET from the 1960s to the 1980s introduced fundamental concepts of packet switching and dispersed networking, leading to the adoption of Transmission Control Protocol/Internet Protocol [TCP/IP] in military networks, marking a shift toward more reliable systems (Saide, 2024).

Emergence and Application of SDN in Tactical Environments

Software-Defined Networking, initially developed for data centers in 2008, introduced key innovations, including the separation of the control and data planes, centralized network intelligence, and programmable interfaces (Kamboj & Pal, 2021). These features help solve the problems faced by military networks, especially the need to quickly adjust and use resources effectively in challenging situations. The motivation for SDN adoption in tactical networks stems from several key requirements:

- Flexible, programmable network architectures that can dynamically respond to shifting battlefield conditions.
- Efficient bandwidth and energy management, ensuring optimal use of constrained tactical communication resources.
- Seamless integration of heterogeneous communication technologies, including various radio access methods.
- Enhanced survivability in contested electromagnetic environments, minimizing vulnerabilities to cyber and electronic warfare threats.
- Gradual transition from legacy systems, allowing phased implementation without disrupting existing military communication frameworks.

The SDN-based architectural models vary from small upgrades to current systems to full replacements of old routers with SDN switches, providing different options for implementation based on what is needed for operations. The use of SDN in military networks marks a major change in how communication happens on the battlefield, making it easier to adapt quickly, stay strong during operations, and manage data traffic more precisely in changing situations. Hybrid architectures that use SDN principles can help make gradual changes, while methods for discovering network layouts improve understanding of the situation and make better use of resources in challenging environments.

Enhanced Tactical Communication Network Architecture for Resilience and Mobility

Tactical Communication Networks [TCNs] are the fundamental framework for contemporary battlefield communication, connecting mobile nodes [MNs] and intermediate nodes [INs] to enable real-time exchange of data (Elmasry, 2012). These networks leverage a combination of point-to-point and point-to-multipoint wireless transmission modes, guaranteeing adaptability in network deployment while preserving operational efficiency in changing environments. Nonetheless, battlefield conditions present ongoing challenges—enemy attacks may partially or entirely incapacitate essential INs, disrupting connectivity and impairing situational awareness. Ensuring service continuity for disconnected mobile nodes necessitates effective countermeasures, incorporating sophisticated mobility management mechanisms and resilient routing systems.

Network Adaptation Strategies for Disrupted Tactical Environments

The shift from IPv4-based TCNs to IPv6 has improved scalability, security, and address allocation efficiency, enabling military networks to accommodate larger, more dynamic force

structures. Due to the requirement for prompt and precise data transfer, mobility management becomes a crucial facilitator of network resilience. Various frameworks have been examined to enhance MN interoperability and communication within battlefield limitations:

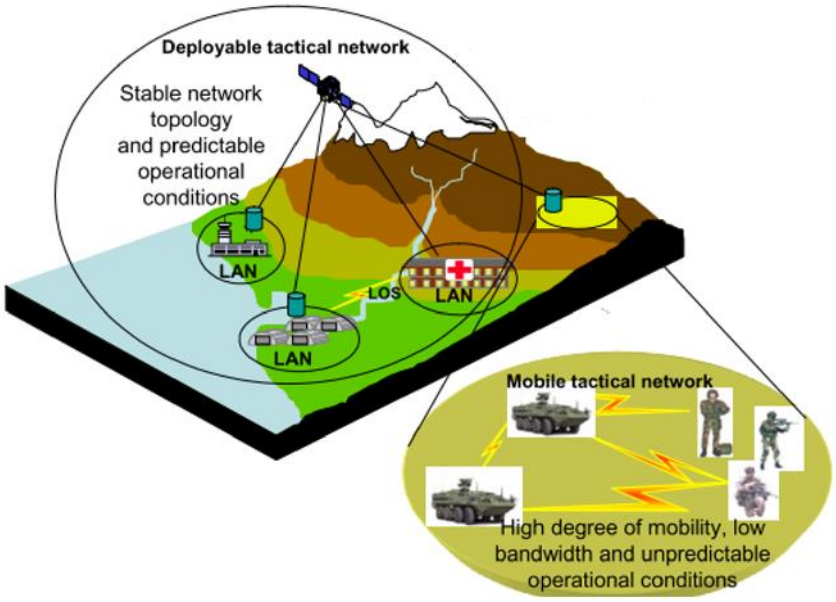
- *Integration of Mobile IPv6 [MIPv6]:* several works have validated the practicality of MIPv6 in tactical network implementations, facilitating uninterrupted mobility management while preserving data integrity (Dutta & Sarma, 2022).
- *Network Mobility [NEMO] Protocols:* Hybrid architectures that integrate MIPv6 and NEMO facilitate coordinated group mobility, enhancing synchronization across deployed MNs and minimizing handover delay.
- *Centralized Routing Optimization:* A suggested integrated satellite-terrestrial paradigm features a central authority to manage routing decisions, guaranteeing efficient communication channels despite intermittent connectivity.
- *Enhancements to Proxy Mobile IPv6 [PMIPv6]:* Developed to address the constraints of Mobile IPv6 [MIPv6], PMIPv6 reduces signaling overhead and improves scalability. Nevertheless, vulnerabilities like single-point failures at anchor nodes provide security risks that necessitate mitigating techniques.

Advanced Mechanisms for Tactical Mobility Management

As operational risks evolve, the management of mobility in Tactical Communication Networks must incorporate real-time adaptive frameworks, enhanced interference mitigation strategies, and seamless communication across diverse regions to maintain critical connections. Future enhancements will focus on developing networks capable of self-adjustment, utilizing AI to adjust mobile node connections in response to environmental changes and interference from adversaries. These intelligent network systems will employ data analysis and machine learning techniques to facilitate rapid decision-making, enhance communication pathways, minimize delays, and mitigate traffic congestion.

To enhance reliability during node failures and address competition for radio frequencies, multi-homed tactical networking employs a combination of satellite communications [SATCOM], terrestrial RF mesh networks, and directional beamforming technologies to ensure data integrity and redundancy. Integrated network solutions provide the dynamic adjustment of workloads and frequency modulation, ensuring operational stability even in rapidly evolving battlefield conditions. Sophisticated communication systems enhance mission performance and adaptability in tough circumstances by facilitating seamless collaboration between dependable network architectures and mobile tactical networking, as illustrated in Figure 3.

Figure 4.3: *Illustration of the Integration between Stable Network Topologies and Mobile Tactical Networking through SATCOM Systems.*

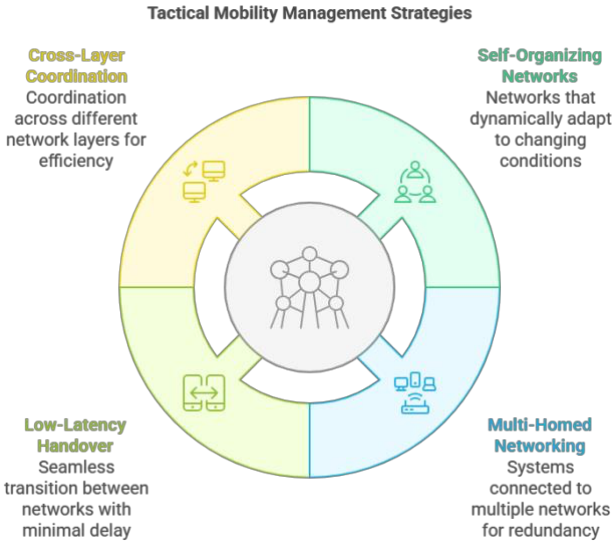


Source: *adapted from* Fagervoll (2017)

Tactical mobility management techniques must facilitate seamless coordination among the physical, network, and application levels, enabling diverse systems to operate cohesively and maintain robustness, as seen in Figure 4. These strategies will emphasize adaptable network control systems, rapid resolutions for interference problems, and autonomous synchronization techniques to enhance defense against cyber threats and disturbances in the electromagnetic spectrum. Moreover, multi-path routing and frequency agility approaches will enhance communication stability, allowing military units to function efficiently in contested areas.

The implementation of these innovations will enhance military communication infrastructures, ensuring real-time adaptation and uninterrupted service under changing battlefield conditions, while strengthening mission-critical communications against potential disruptions.

Figure 4.4: *Tactical Mobility Management Strategies.*



Network Architecture for Resilience

The robustness of military networks is fundamentally rooted in their architectural design, which must endure disasters, hostile disturbances, and advancing technical challenges. This section examines critical design concepts that enhance network resilience, emphasizing decentralized structures, cross-domain functionality, and innovative technologies that facilitate rapid adaptation and threat management. Tactical communication networks must continually adapt to cope with new issues arising from network failures, cyber threats, and adversary jamming methods. Although existing mobility management systems like as MIPv6, PMIPv6, and NEMO offer significant advantages, further enhancements are necessary—such as adaptive AI, advanced security protocols, and dependable mesh networking concepts—to guarantee seamless operation.

Distributed Network Topologies

Distributed network architectures eliminate single points of failure, ensuring robustness and adaptability under diverse operational conditions. Military networks increasingly adopt mesh, hierarchical, and hybrid topologies that dynamically reconfigure based on threat conditions and mission requirements.

Mesh Networks

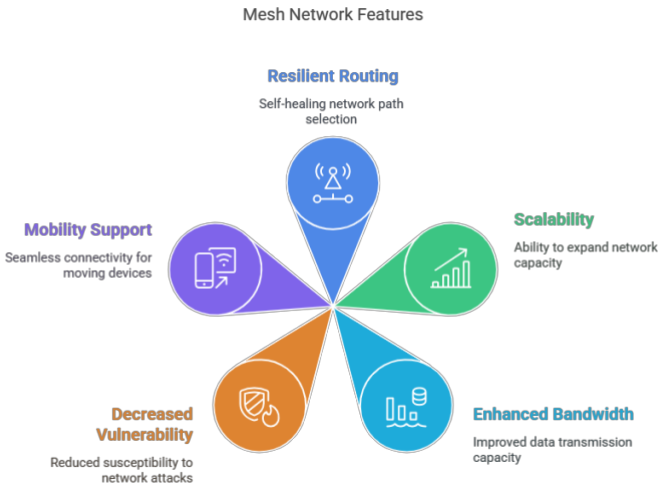
Mesh networks play a critical role in tactical communication systems by establishing multiple redundant communication routes between different nodes, as shown in Figure 5. Furthermore, their decentralized architecture enhances network resilience by enabling dynamic

rerouting of data in response to disruptions, or weak communication, and therefore ensuring operational continuity in unpredictable and hostile environments. Additionally, their scalable design allows seamless integration of new nodes without reliance on centralized infrastructure or human intervention, facilitating the whole network adaptability in mission-critical scenarios.

To optimize the performance of military mesh networks, key considerations include efficient power management, advanced routing algorithms, and robust interference mitigation techniques to maintain reliable connectivity under diverse operational conditions.

Military mesh networks become more flexible through the use of software-defined networking, enabling quick changes according to mission requirements. By leveraging SDN-based control mechanisms, tactical forces can optimize resource allocation, enhance situational awareness, and improve mission responsiveness. These advancements collectively reinforce the reliability of military communication infrastructures, ensuring sustained operational effectiveness in hostile environments.

Figure 4.5: *Mesh Network Features.*



Hierarchical Networks with Redundancy

Hierarchical military network architectures match traditional command structures, with higher-level nodes needing more bandwidth and backup systems to support command and control [C2] functions. These networks incorporate multi-tiered redundancy mechanisms, ensuring operational survivability by maintaining backup nodes across various levels of command. Additionally, connections between different levels of the hierarchy provide two ways to stay connected, strengthening communication between command centers and tactical units.

Strategic plans establish backup command systems to ensure communication even if primary nodes fail. Tactical networks rapidly adapt to challenges, maintaining mission continuity. Edge computing reduces central reliance, enabling decentralized decision-making and real-time data processing. This enhances responsiveness, lowers latency, and strengthens adaptability, allowing military units to make informed decisions and react swiftly in dynamic battlefield scenarios.

Multi-Domain Network Integration

Modern military networks encompass various domains—land, sea, air, space, and cyber—requiring communication infrastructures that are both interoperable and resilient. Effective integration across these domains facilitates seamless data exchange and ensures secure command coordination in diverse operational environments.

Cross-Domain Solutions [CDS]

Cross-domain solutions are essential for the secure transmission of information between networks that have various security classifications. These systems employ multi-tiered security techniques to impose detailed access rules, guaranteeing that only authorized individuals can access sensitive information. Protocol mediation and data filtering methods filter information transmissions, minimizing the possibility of illegal data leakage.

High-assurance security protocols, such as unidirectional communication, enable regulated data transfer into higher-security environments, obstructing forbidden bidirectional access. Contemporary cross-domain solutions progressively integrate Zero Trust Architecture [ZTA], enforcing ongoing identity verification and rigorous access validation to safeguard against insider risks and external cyber threats (Phiayura & Teerakanok, 2023; Nahar et al., 2024; Sasada et al., 2023; Tsai et al., 2024).

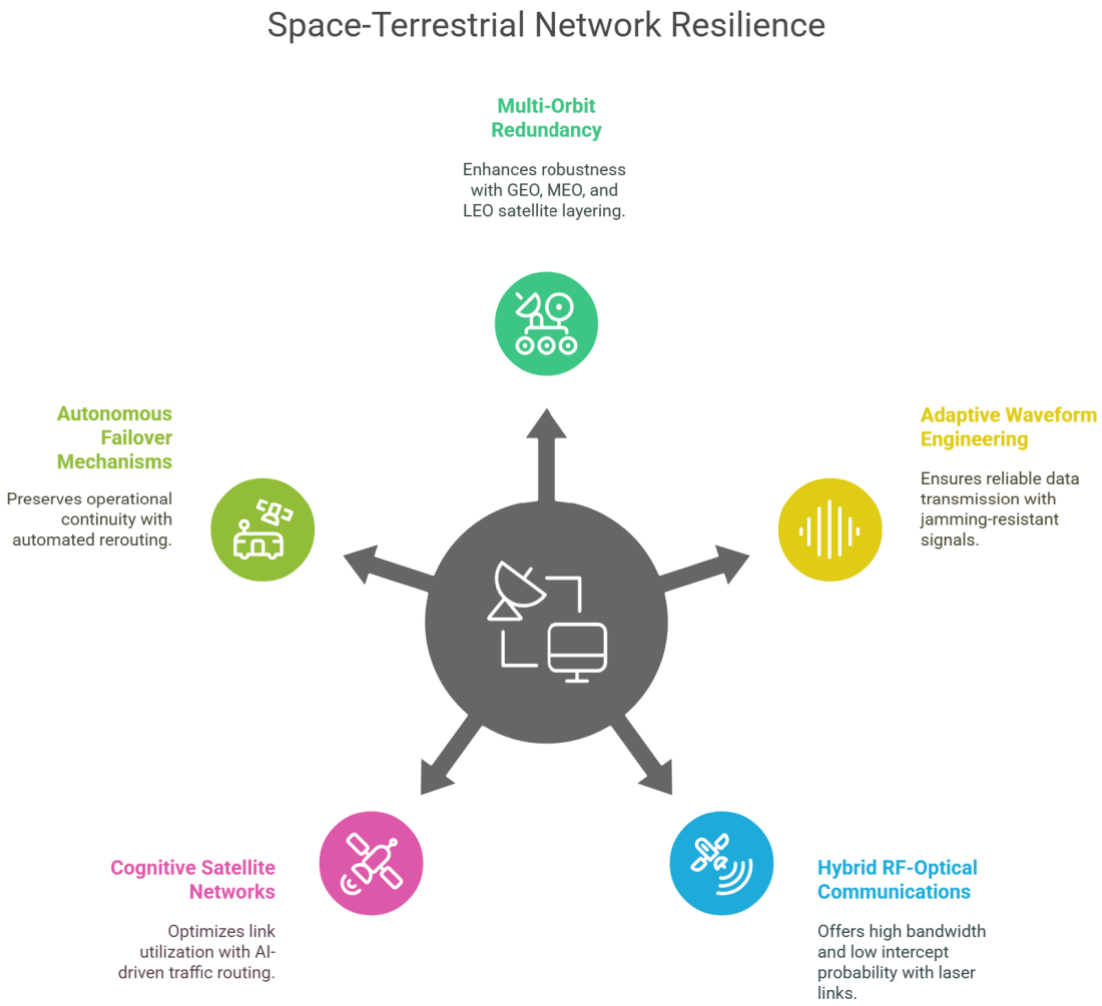
Space-Terrestrial Network Resilience

Satellite communication networks are essential for military communications by providing global coverage, secure communication, and emergency systems that enhance operational efficiency under difficult ground conditions. The combination of space-based and terrestrial infrastructures guarantees dependable command and control operations, and therefore, preserving mission continuity even in adversarial electromagnetic circumstances (Fagervoll, 2017).

Multi-orbit redundancy, employing geostationary [GEO], medium earth orbit [MEO], and low earth orbit [LEO] satellites concurrently, enhances communication reliability. Advanced signal processing techniques might enhance transmission by employing methods that resist jamming, thereby securing against electronic warfare disruptions. For example, hybrid radio frequency [RF]-optical communication systems use space-based laser links to facilitate rapid and secure data transmission, hence enhancing the safety of military communications.

Cognitive satellite networks employ artificial intelligence to regulate data traffic and enhance connectivity, rapidly adapting to interference and cyber threats in real-time. Autonomous backup systems between terrestrial and satellite networks might ensure connectivity by automatically identifying alternative route in the event of disruptions to primary communication links. The integration of these technologies provides a highly adaptable and secure military communication system, essential for mission-critical operations across various domains. Figure 6 illustrates the notion of Space-Terrestrial Network Resilience alongside a multi-tiered satellite system comprising both GEO and LEO satellites. The users in this system comprise airborne and terrestrial vehicles and gadgets, including ships. The GEO satellite provides comprehensive coverage of the entire region, whereas the LEO satellites concentrate on particular sites.

Figure 4.6: *Space-Terrestrial Network Resilience.*



Expanding the Role of the Internet of Military Things

The modern battlefield increasingly depends on real-time intelligence, autonomous decision-making, and interconnected combat technologies, highlighting the essential function of the Internet of Military Things [IoMT] and its subset, the Internet of Battlefield Things [IoBT]. These frameworks represent a sophisticated model of ubiquitous computing, incorporating distributed sensors, actuators, and intelligent systems spanning terrestrial, maritime, aerial, and cyber domains to enhance military operations, reconnaissance, and combat efficacy.

IoMT Architecture and Distributed Systems

The Internet of Military Things [IoMT] combines sophisticated sensors, intelligent communication networks, and real-time data processing to enhance command and control [C2] operations. Through the utilization of edge computing, AI-driven analytics, and cyber-physical systems, the Internet of Military Things [IoMT] facilitates autonomous decision-making, adaptive

mission planning, and seamless coordination within changing battlefield conditions. IoMT-enabled operations enhance situational awareness by using connected sensors and self-operating systems, providing ongoing updates for intelligence, surveillance, and reconnaissance [ISR]. AI-driven predictive risk assessment further strengthens strategic decision-making by analyzing battlefield dynamics, detecting emerging threats, and recommending adaptive tactical responses in real time (van Niekerk, 2021). For instance, the U.S. Department of Defense's Project Maven (*the Algorithmic Warfare Cross-Functional Team*) was launched in 2017 to integrate machine learning and computer vision into the analysis of full-motion video from unmanned aerial systems. By automating the detection and tracking of objects of interest, the system reduces analysts' workload and shortens the sensor-to-decision cycle, which allows commanders to make faster and more informed tactical decisions in IoMT-enabled command frameworks (Hogue, 2021).

Unmanned aerial, terrestrial, and maritime systems are essential for reconnaissance, precise targeting, and operational adaptability, enhancing mission execution with limited human involvement. Furthermore, wearable and biometric technology, such as smart devices, exoskeletons, and health-monitoring systems, electrocardiogram (*ECG or EKG*), temperature monitoring, localization, augment military preparedness, efficacy, and survival in critical emergency situations. Smartwatches can monitor a soldier's heart rate and body temperature in real-time and immediately signal potential physical distress or injury to a command center. Similarly, the integration of gas sensors into helmets can provide early warnings of chemical threats in the environment and allow soldiers to take protective measures.

IoMT and Cyber Warfare: Intelligence-Driven Combat Operations

Improvements in autonomous warfare technology enable machines to handle tasks in cyber defense, drone missions, and robotic soldier support, which lowers the need for human involvement in dangerous situations and makes operations more efficient. Also, AI-powered electronic warfare tools strengthen cyber-electromagnetic dominance by countering enemy jamming, misleading signals, and cyber attacks. These combined technologies are essential for developing warfare strategies that focus on quickly adapting to changes and automatically handling threats. For instance, sophisticated spoofing attacks, which involve injecting falsified navigational data, have become easier to execute over a short period. They allow attackers to influence GPS-users or systems for their benefit. The miniaturization and versatility of software-defined radios [SDRs] and computer systems like the Raspberry Pi have made it possible to create low-cost, portable, and concealable spoofing devices that can affect multiple receivers. These advancements allow for smooth takeover attacks where signals are synchronized and gradually

overpower original ones, effectively "hypnotizing" a system or fooling a person with incorrect information (Westbrook, 2025). In the context of the Ukraine conflict, Starlink terminals formed an ad hoc IoMT backbone for Ukrainian forces. They enabled distributed units to coordinate strikes, conduct ISR, and maintain command and control even in the face of widespread infrastructure disruptions.

Despite its transformative potential, IoMT presents challenges related to cybersecurity vulnerabilities, interoperability complexities, and bandwidth constraints, necessitating continuous refinement. Future research needs to focus on improving security for military digital systems by developing new ways to protect against advanced cyber threats, using AI for better cyber defense, ensuring safe data sharing with blockchain, and creating networks that can operate independently.

Communication Technologies for Hostile Environments

Military operations in adversarial environments necessitate sophisticated communication technology intended to maintain performance in challenging circumstances. These systems must withstand electromagnetic interference, adversary jamming, physical disruptions, and infrastructure deterioration to maintain continuous communication across operating theaters. This section examines significant advancements in resilient military communications, such as robust radio frequency [RF] transmission, beyond-line-of-sight [BLOS] transmission technologies, and alternative communication frameworks that improve operational survival in disputed environments.

Resilient Radio Frequency [RF] Systems

Radio frequency [RF] communications remain the backbone of tactical military networks, offering high mobility, adaptability, and rapid deployment capabilities. Advanced RF systems integrate frequency agility, anti-jamming techniques, and secure waveforms to mitigate adversarial disruptions while ensuring operational effectiveness (Chai et al., 2014).

Frequency Agility and Spectrum Management

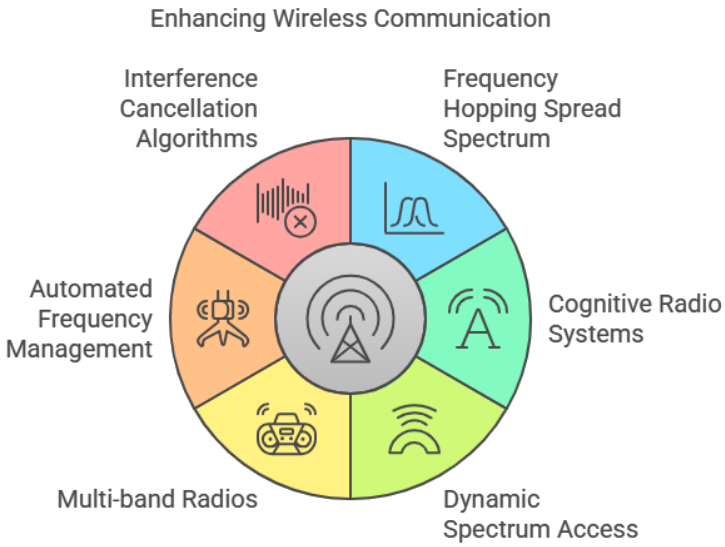
Modern military RF systems use adaptive spectrum management to guarantee secure and stable communications in dynamic environments influenced by interference and electronic warfare [EW]. Frequency Hopping Spread Spectrum [FHSS] reduces jamming threats by rapidly shifting transmission frequencies, whereas cognitive radio utilizes AI-based spectrum sensing to enhance channel selection and signal quality (Kirk et al., 2023).

Dynamic Spectrum Access [DSA] improves bandwidth efficiency by enabling opportunistic spectrum allocation, hence reducing congestion in coalition operations. Multi-band radios facilitate

interoperability among tactical, aerial, naval, and space-based groups, guaranteeing uninterrupted communication. Automated frequency management coordinates networks, reducing interference and mitigating risks such as jamming and spoofing.

Interference cancellation algorithms enhance spectral efficiency by dynamically adjusting transmission configurations in real time. These combined strategies enhance military RF resilience, ensuring reliable communications in disputed conditions. Figure 7 illustrates the optimization of wireless communication and frequency management in tactical networks, highlighting the interplay between dynamic spectrum adaptation, interference mitigation, and real-time synchronization mechanisms.

Figure 4.7: *Optimization of Wireless Communication and Frequency Management in Tactical Networks.*



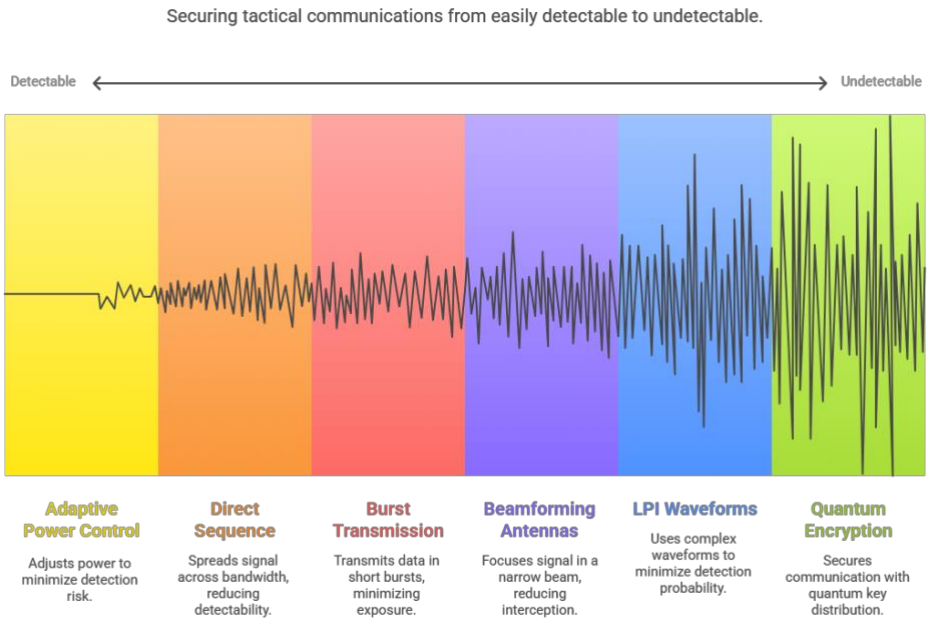
Anti-Jam Communications in Tactical Networks

Ensuring the protection of military communications from intercepting and jamming requires advanced technologies and adaptive techniques. On the one hand, Direct Sequence Spread Spectrum [DSSS] improves robustness by dispersing signal energy over many frequencies, hence minimizing interference concerns while maintaining data accuracy. On the other hand, adaptive power control dynamically modifies transmission strength according to external factors, hence reducing detection by attackers and limiting the effectiveness of adversarial jamming.

Figure 8 depicts defensive measures, including detectable strategies solutions that guarantee efficiency. Quantum encryption, using quantum key distribution [QKD] for example,

offers superior safety through using quantum entanglement to prevent unauthorized access. QKD enables the generation of cryptographic keys that are virtually immune to eavesdropping, as any interception attempt disturbs the quantum state and is immediately detectable. As quantum security frameworks advance, they will be essential in protecting military communication networks from cyber-electromagnetic threats (Cao et al., 2022; Biswas et al., 2022; Ricci et al., 2024).

Figure 4.8: *Securing tactical communication from easily detectable to undetectable.*



However, despite its potential, the scalability of quantum encryption remains a critical challenge. Current QKD implementations are limited by photon loss and noise in quantum channels, which degrade the signal and reduce effective communication distance, typically operating over distances up to several hundred kilometers. To overcome these distance limitations, quantum repeaters are being developed, but their integration into existing classical networks requires sophisticated hardware and protocols. Furthermore, the specialized equipment required for QKD is expensive and complex to deploy, leading to high infrastructure costs. Moreover, satellite-based quantum communication, while promising for long-distance transmission, faces constraints related to signal attenuation, weather conditions, and orbital limitations. Efforts are underway to develop more cost-effective and robust quantum communication technologies and to integrate QKD with existing classical communication networks through hybrid systems (Sahu & Mazumdar, 2024). For tactical military environments, especially

those characterized by mobility, contested terrain, and rapidly changing topology, the integration of QKD may not yet be operationally feasible.

Beyond Line-of-Sight [BLOS] Communications

Long-range military operations often necessitate BLOS communication technologies to bypass terrain obstructions, sustain connectivity across dispersed units, and provide redundancy in disrupted networks.

High Frequency [HF] Communications

High-frequency [HF] radio communications, which work in the 3–30 MHz range, use reflections from the ionosphere to send signals over long distances between continents without needing satellites. This capability is especially important for maintaining strong communication connections in situations where satellite access might be blocked or weakened by electronic attacks or natural events.

Advancements in HF radio technology have significantly enhanced tactical communication effectiveness. Automatic Link Establishment [ALE] protocols help choose the best frequencies for clear communication even when the ionosphere changes, and wideband HF technology increases the amount of data that can be sent, allowing speeds over 120 kbps for better performance (Wu et al., 2020). Third-generation HF protocols make signals stronger by using smart coding and better error correction methods, which help reduce interference and signal loss in challenging situations.

Near Vertical Incidence Near Vertical Incidence Skywave [NVIS] propagation allows secure communication without needing a direct line of sight, helping forces stay connected in areas with obstacles or when facing jamming from enemies (Dear et al., 2024). Furthermore, integrating IP-based HF networks enables seamless interoperability between legacy radio systems and modern battlefield data architectures, enhancing cross-branch coordination and operational efficiency. These advancements will reinforce HF radio as a critical asset in military communication strategies, ensuring reliable connectivity where conventional networks may be compromised.

Ultra-high frequency [UHF] and super high frequency [SHF]

Ultra-High Frequency [UHF] and Super High Frequency [SHF] communication technologies allow signals to be sent over medium distances (*50–300 km*) by bouncing off the atmosphere, ensuring reliable connections without needing satellites. Such improvements in frequency use bands have increased bandwidth capacity, facilitating encrypted data transmissions

of up to 40 Mbps, while adaptive modulation and error correction methods enhance signal robustness under diverse settings.

Modern beyond-line-of-sight [BLOS] communication systems, integrated with satellite and terrestrial networks, adapt dynamically to mission requirements. Anti-jamming techniques, such as frequency-hopping spread spectrum [FHSS] and adaptive beamforming, enhance resistance against electronic warfare, ensuring secure command and control operations in contested environments.

Alternative Communication Bearers for Operational Redundancy

To mitigate connectivity disruptions from adversarial attacks, environmental conditions, and infrastructure degradation, military networks incorporate non-RF communication modalities that provide strategic redundancy (Chehri et al., 2023; Abd El-Mottaleb et al., 2024; Abd El-Mottaleb et al., 2023).

Optical and Laser Communications

Free-space optical [FSO] and laser communication technologies provide rapid and secure data transmission, enhancing the safety of military communications in environments with significant electronic interference. These technologies employ high-speed optical lines, ranging from 1 Gbps to 100 Gbps, to provide real-time intelligence, surveillance, and reconnaissance [ISR] operations. In addition, such changes will enable critical information to transfer seamlessly on the battlefield without reliance on congested radio frequencies.

The focused laser communication beam significantly diminishes the likelihood of signal interception, hence enhancing security by lowering the risk of unwanted detection and exploitation by adversaries. Furthermore, FSO systems are inherently secured against RF jamming, electronic warfare interruptions, and frequency congestion. These optical transmission methods do not require conventional spectrum licensing, enabling their unrestricted usage in tactical scenarios to assist both mobile and stationary military assets (Mansoor et al., 2024).

Despite their advantages, optical communication networks may be less effective due to atmospheric signal absorption, scattering, and adverse weather conditions—such as fog, rain, and dust storms—necessitating the integration of RF and optical systems with complex correction techniques (Chehri et al., 2023; Abd El-Mottaleb et al., 2022a; Abd El-Mottaleb et al., 2022b; Abd El-Mottaleb et al., 2022c; Zeghid et al., 2021).

Acoustic and Seismic Communications

Acoustic communication systems provide excellent options for safely sending data in situations where enemy interference makes using electromagnetic waves difficult or impossible.

Underwater acoustic communication networks are crucial for military operations involving submarines, using low-frequency sound signals to send data over long distances with little power while reducing signal loss in the ocean. Similarly, through-earth seismic transmission systems allow signals to travel secretly underground and in closed spaces, making sure military communications stay secure in places like caves, tunnels, and strong underground buildings.

In disaster management, seismic sensor networks facilitate discreet building communications through vibrations, reducing electronic detection risks while ensuring operational security. Furthermore, emergency communication systems that are designed for disaster management and rescue operations utilize sound- and vibration-based methods to maintain connectivity during crisis scenarios. These systems enhance first responders' ability to coordinate rescue missions, for earthquake rescue, for example, ensuring stable communication in environments where traditional networks may be disrupted. Additionally, in disaster-stricken areas, resilient seismic and acoustic messaging enables rapid response efforts, supporting evacuation protocols and emergency coordination.

Figure 9 provides a comparative analysis of communication systems, detailing their designs, power requirements, security features, costs, and other operational parameters. Figure 10 complements this by comparing how different communication technologies stack up against each other by checking factors like delay, data transfer speed, ability to adjust frequencies, resistance to interference, and how well they work with modern networking systems, making sure to thoroughly evaluate how well they meet various mission requirements. Together, these figures support informed decision-making by aligning system capabilities with the specific demands of diverse operational environments.

Figure 4.9: *Communication Systems in Perspective: Contrasting Technical Capabilities and Applications.*

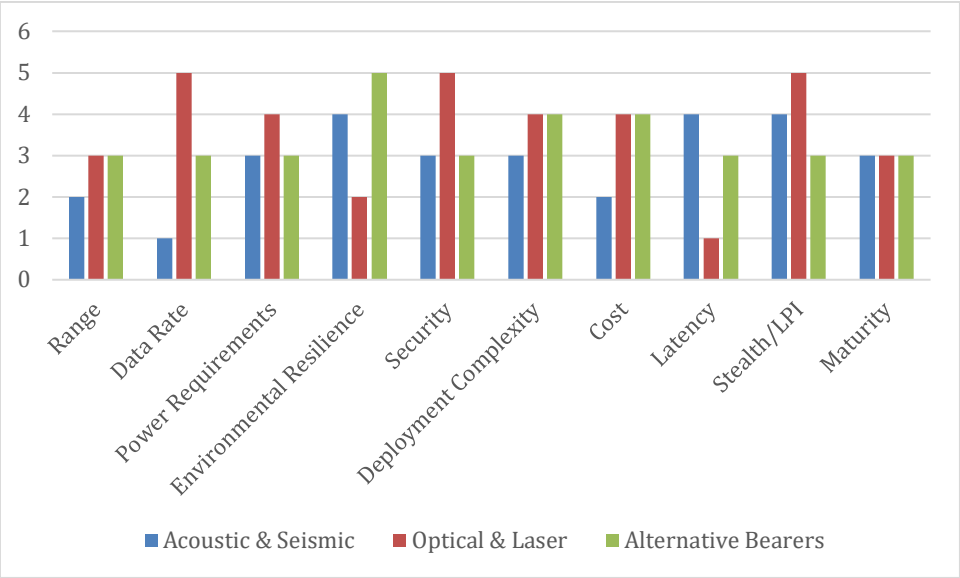
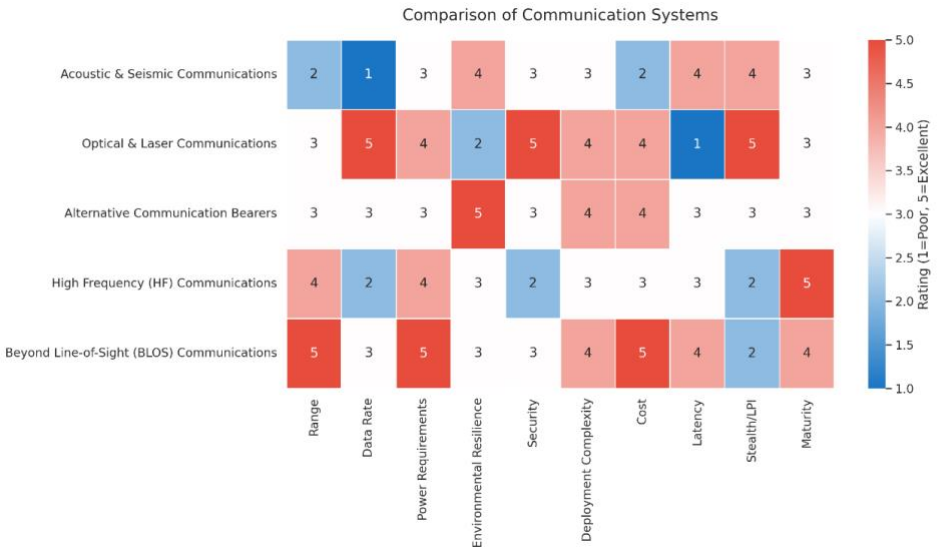


Figure 4.10: *Evaluating Communication Systems: A Comparative Analysis of Technologies and Performance.*



Strategic Research Directions in Military Communications

Future advancements must focus on post-quantum encryption for secure communications, AI-optimized spectrum resilience, and hybrid multi-domain integration to ensure persistent, adaptive connectivity across contested battlefields. Emerging developments include AI-powered autonomous network self-healing mechanisms, biologically inspired sensor architectures (El Ouahmani et al., 2019), and blockchain-secured tactical communication protocols to further

enhance network robustness (Lazrag et al., 2021; Chaibi et al., 2025; Ababio et al., 2025; Kumar Jagatheesaperumal et al., 2025; Riaz et al., 2025; Lazrag et al., 2019).

Cybersecurity and Information Assurance

Cybersecurity is a fundamental pillar of military network resilience, safeguarding operational integrity against cyberattacks, electronic warfare, and advanced persistent threats [APTs] (Quadar et al., 2022). To ensure protection, tactical military networks must integrate multi-tiered security frameworks that uphold confidentiality, integrity, and availability (*CIA triad*) across defense systems.

However, traditional castle-and-moat security models introduce some vulnerabilities and therefore enable lateral movement attacks that allow adversaries to escalate privileges once inside the perimeter. Consequently, modern military systems have recently transitioned to Zero Trust [ZT] security principles, enforcing continuous authentication and strict identity validation at every network interaction. One key characteristic of this approach is integrating multiple advanced security layers to maintain comprehensive defense (Ahn et al., 2024).

Additionally, mission-focused micro-segmentation, using software-defined networking, stops unauthorized access by separating traffic according to what is needed for operations. Stateful firewalls provide granular data flow control within segmented network sections, restricting unauthorized users from reaching sensitive information. Additionally, Software-Defined Perimeters [SDP] employ dynamic encrypted tunnels, effectively obfuscating critical network assets from external detection and intrusion attempts. To further strengthen security, continuous authentication methods—such as Multi-Factor Authentication [MFA], fingerprint verification, and security tokens—ensure strict access control enforcement (Alquwayzani & Albuali, 2024).

Furthermore, least privilege enforcement strategies use just-in-time [JIT] provisioning to give access only when it's needed, which helps reduce the risk to sensitive resources. Meanwhile, encryption techniques like MACsec [IEEE 802.1AE] and IPsec with Perfect Forward Secrecy [PFS] secure inter-network communications, preventing data theft or tampering. As discussed in *Anti-Jam Communications in Tactical Networks*, quantum encryption, particularly quantum key distribution [QKD], offers promising protection against future cyber-electromagnetic threats.

Endpoint security is also crucial, especially in contested or degraded environments. Host-Based Intrusion Prevention Systems [HIPS] provide kernel-level monitoring, neutralizing rootkits, ransomware, and memory injection attacks before they compromise operational integrity. Additionally, cryptographic validation techniques ensure secure software execution by restricting unauthorized alterations to mission-critical applications.

By employing a multi-tiered security architecture, military networks systematically integrate diverse defensive strategies to minimize system-wide failures. This layered approach maintains proactive defense against nation-state entities, cybercriminal groups, insider threats, and automated cyberattacks.

For operational continuity, military networks require a comprehensive cyber threat detection and incident response strategy that integrates advanced security monitoring systems, threat intelligence fusion, machine learning-driven analytics, and adaptive defense mechanisms. Given that sophisticated attackers, including state-sponsored hackers and autonomous attack frameworks, continuously evolve their techniques, real-time threat monitoring, proactive threat hunting, and automated response mechanisms are vital to mitigating cybersecurity risks before they affect mission-critical systems. As military operations increasingly depend on resilient network infrastructures, next-generation cybersecurity advancements must evolve and focus on autonomous threat mitigation, quantum-resistant encryption, and AI-driven resilience frameworks to preserve operational integrity across contested battlefields.

Finally, secure information exchange within coalition and multi-domain operations demands blockchain-based cybersecurity frameworks. Distributed ledger technologies enhance data integrity, mission-critical asset tracking, and tamper-proof authentication mechanisms, reinforcing cryptographic trust across classified communication networks. Additionally, permissioned blockchain systems make it easier for different agencies to work together and keep command-and-control [C2] operations in sync, ensuring that important cyber intelligence stays safe from unauthorized changes.

Power and Energy Resilience

Reliable and robust power infrastructure is crucial for maintaining military network operations, especially in situations when commercial power grids may be disrupted by natural catastrophes, hostile acts, or logistical limitations. Consequently, ensuring continuous operation necessitates a synthesis of backup power systems, advanced power management tools, energy-efficient strategies.

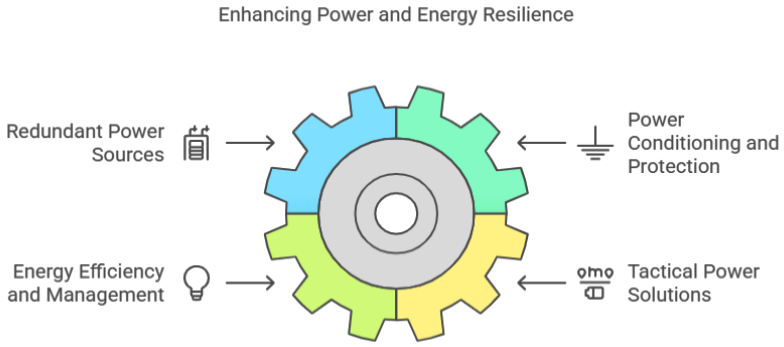
Military networks depend on redundant power sources to maintain operational continuity during primary energy outages. Commercial grids function as the foundation in stable settings; however, military stations must have contingency strategies, including diesel generators with operational capacities over 72 hours to ensure emergency backup during longer outages. Moreover, Uninterruptible Power Supplies [UPS] facilitate uninterrupted transitions between power sources, averting interruptions to essential command and control systems.

Moreover, renewable energy solutions, such as solar panels with integrated battery storage, provide sustainable options that reduce reliance on fossil fuels while improving operational resilience in remote or challenging areas (Mohamed et al., 2019; Chatterjee et al., 2019). Advanced fuel cell systems offer silent, efficient energy production with reduced thermal and acoustic signals, enhancing stealth in forward-operating bases. Under optimal conditions, wind turbines provide additional energy production, enhancing the resilience of off-grid networks. Moreover, tactical vehicle-based power distribution allows mobile units to generate and disseminate electricity, guaranteeing connectivity in field operations independent of permanent infrastructure.

Additionally, hybrid power systems, combining renewable and conventional energy sources, provide adaptable energy inputs based on available conditions. Tactical microgrid systems enhance resilience at forward-operating bases by integrating decentralized energy nodes for localized power generation. Energy scavenging technologies further contribute by harvesting energy from environmental sources, such as movement, temperature differentials, and solar radiation, to sustain networks without requiring continuous fuel supplies.

Wearable power sources equip individual soldiers with portable energy solutions that support personal communication devices and electronic warfare tools. Rapid-deployment solar-battery systems provide emergency energy support for critical military missions, ensuring operational stability under urgent conditions. Figure 11 presents an overview of techniques designed to enhance power and energy resilience.

Figure 4.11: *Enhancing power and energy resilience.*



Tactical Communication Systems in Disaster Response

The first few hours following a disaster are crucial for an effective response, requiring sophisticated military communication systems intended for rapid deployment in harsh conditions. Tactical satellite communications [TACSAT] provide beyond-line-of-sight connectivity to maintain operational capabilities, especially when terrestrial infrastructure is impaired.

During Hurricane Maria in Puerto Rico (2017), more than 95% of cell towers were destroyed, leaving standard communication networks ineffective. In response, military TACSAT systems restored connections within 48 hours, facilitating relief coordination across 12 localities. This permitted medical evacuations, logistical coordination, and supply distribution, illustrating the strategic significance of TACSAT in military and humanitarian operations (Gómez-Fragoso et al., 2022).

Furthermore, military disaster response increasingly relies on collaborative communication tools that improve coordination and guarantee interoperability between military and civilian responders. To meet this requirement, deployable 5G/LTE networks provide connectivity in locations with severely compromised infrastructure, while unified command post systems incorporate secure virtual networks that provide differentiated access management for various organizations. Moreover, real-time operational intelligence technologies enhance situational awareness, facilitating effective decision-making. For example, during the California wildfires of 2018 and 2024, Disaster Response Communications [DRC] packages assisted National Guard units by enabling interoperable voice communications and coordinated resource tracking.

Moreover, airborne communication devices enhance disaster response by ensuring connectivity in isolated and compromised regions. High-altitude platforms provide extensive coverage, frequently surpassing a 100-mile radius, while multi-band relay systems promote cross-agency interoperability, allowing military, firefighting, and disaster management teams to maintain uninterrupted contact. Simultaneously, unmanned aerial vehicles [UAVs] augment surveillance

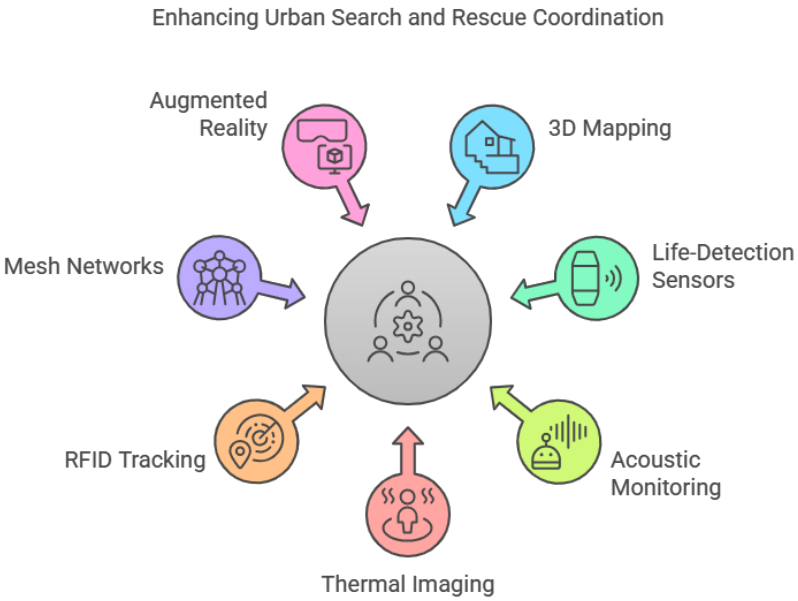
capabilities by monitoring fire advancement and detecting imminent hazards. Additional meteorological monitoring stations provide essential wind speed and directional data, aiding in the prediction of fire behavior and the enhancement of response plans. Moreover, satellite imagery facilitates extensive study by monitoring the progression of fires over time, providing critical insights on containment strategies and long-term impact evaluations.

In the case of flood rescue operations also depend on amphibious and maritime communication networks that incorporate waterproof tactical radios for secure messages under harsh conditions. Underwater acoustic communication systems could facilitate submerged infrastructure evaluations, allowing professionals and emergency responders to assess structural integrity in flooded conditions.

Similar in importance, earthquakes pose unique challenges to emergency communications due to the unexpected and extensive devastation of infrastructure, frequent aftershocks, and complex urban search and rescue operations. Military tactical networks enable prompt evaluations of structural damage, compromised transportation routes, and failures in essential infrastructure to aid quick reaction actions. Utilizing autonomous sensing technology, UAVs fitted with automated damage detection software acquire real-time imagery, promptly recognizing collapsed structures and blocked routes. Furthermore, helicopters equipped with LiDAR accurately map structure deformations, providing critical engineering data for reconstruction design. In the 2023 Turkey-Syria earthquake, armed troops utilized modern technologies, including ground-penetrating radar and real-time structural analysis, to evaluate structure stability (FEMA, 2018; U.S. Department of Defense, 2025). AI-enhanced reconnaissance technologies improved post-earthquake assessments, accelerating recovery efforts and resource distribution.

Additionally, acoustic monitoring systems discover quiet sounds that suggest human presence, enhancing thermal imaging technology that recognize body heat signatures, even in obstructed settings. RFID-based tracking devices enhance operational safety by overseeing the movements of rescue personnel within precarious structures. Mesh networking topologies facilitate communication in degraded radio-frequency settings by extending connectivity into collapsed areas. Augmented reality displays improve situational awareness by delivering real-time hazard notifications and escape route visualizations, enabling rescue crews to navigate disaster sites efficiently. Figure 12 depicts essential technology for urban search and rescue coordination.

Figure 4.12: *Enhancing urban research and Rescue Coordination.*

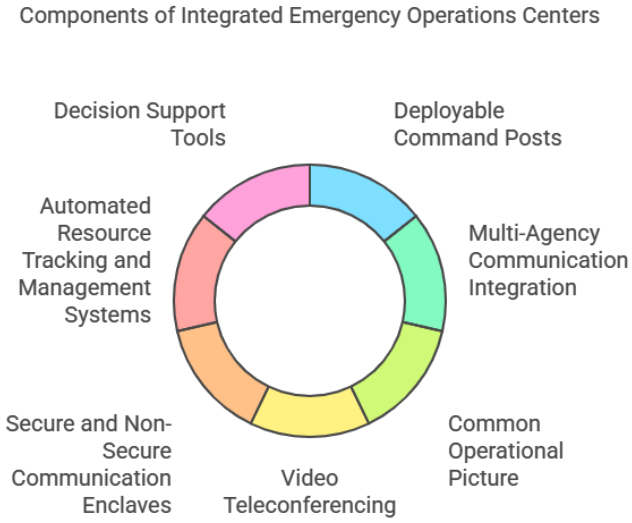


Interoperability is a crucial component of military disaster response networks, facilitating seamless data sharing among military, civilian, and humanitarian organizations while keeping stringent safety precautions. Cross-domain solutions incorporate secure communication frameworks to enable coordinated operations, facilitating real-time information sharing while protecting classified data from unauthorized access.

A unified operational overview compiles situational intelligence, showcasing response resources, risk areas, and emerging threats to improve decision-making. For example, utilizing video teleconferencing systems, distributed command elements could help with coordinating collaboration among geographically separated operational nodes, and therefore facilitating swift adaptations to changing crisis situations. Tactical networks integrate secure and non-secure enclaves to manage access to secret and open-source information, enhancing data integrity and facilitating multi-agency collaboration. Automated resource tracking systems enhance logistical efficiency by offering real-time visibility into human movements, equipment deployment, and supply chain dynamics, hence assuring optimal resource allocation during disaster response operations.

Figure 13 depicts essential functional components of integrated emergency operations centers, highlighting critical technologies that improve interoperability, security, and operational efficacy in disaster management contexts.

Figure 4.13: *Core Functional Elements of Integrated Emergency Operations Centers.*



A notable demonstration of these capabilities occurred during Hurricane Katrina, when military tactical networks were deployed to coordinate the evacuation of over 50,000 civilians from flood-affected regions (INSARAG, 2023; Kemal, 2023). Communication nodes enabled synchronized helicopter and boat rescue operations, tracking evacuation assets and transmitting critical survivor reports to command centers. These networks streamlined the relocation process by matching evacuees with shelters based on medical conditions and family structures, reinforcing military-assisted disaster response efficiency. Ongoing improvements in AI-based prediction tools, self-operating scouting systems, and safe communication methods will make military networks even quicker and more dependable during civilian disaster efforts.

Conclusion

This study provided a comprehensive analysis of military communication networks, focusing on their ability to maintain operational functionality despite environmental and adversarial disruptions. Specifically, it examined the complexities of network architectures, including tactical field communications deployed in combat zones, strategic command and control systems, and theater-wide infrastructures supporting joint operations. The evaluation of military network resilience addressed significant challenges posed by natural disasters and cyber threats, exploring mitigation strategies such as layered encryption protocols, intrusion detection mechanisms, and redundant communication pathways. Additionally, the historical evolution of military

communications highlighted the transformative impact of software-defined networking, improving mobility management and enabling rapid reconfiguration of network architectures.

The study also examined different network designs, including mesh networks for decentralized communication, layered infrastructures incorporating backup systems to enhance reliability, and cross-domain solutions facilitating secure information exchange across multiple security classifications. Similarly, the Internet of Military Things [IoMT] was investigated, underscoring its contributions to network-centric warfare, intelligence-driven combat operations, and cybersecurity defense strategies. Robust communication technologies, including dynamic spectrum management and anti-jam capabilities, were evaluated alongside emerging innovations such as AI-driven automation and quantum-secure encryption techniques. Given these evolving threats, cybersecurity and information assurance are fundamental to resilient military networks, encompassing border defense mechanisms, Zero Trust Architecture-based segmentation, endpoint protection, identity and access management, threat detection, and long-term cyber defense planning.

Additionally, the study explored energy resilience in military networks, particularly through redundant power systems and intelligent energy distribution strategies. Tactical communication solutions for disaster response underscored the importance of interoperability with civilian emergency services. Real-world applications of military communication networks during crises—including wildfires, floods, earthquakes, and other emergency response scenarios—illustrated their adaptability, leveraging airborne communication relays, fire tracking systems, water monitoring technologies, urban rescue coordination frameworks, and integrated emergency operations centers.

By addressing these key aspects, the study established a foundational understanding of resilient military communications, highlighting the ongoing need for innovation in flexible networking, cybersecurity, and interoperable technologies. Future research and strategic advancements will continue shaping the next generation of military communication systems, reinforcing operational effectiveness across contested and disaster-stricken environments.

References

Ababio, I. B., Bieniek, J., Rahouti, M., Hayajneh, T., Aledhari, M., Verma, D. C., & Chehri, A. (2025). A blockchain-assisted federated learning framework for secure and self-optimizing digital twins in industrial IoT. *Future Internet, 17*(1), 13. https://doi.org/10.3390/fi17010013

Abd El-Mottaleb, S. A., Métwalli, A., Chehri, A., Ahmed, H. Y., Zeghid, M., & Khan, A. N. (2022a). New algorithm for a fixed right shift code to support different quality of services in smart and sustainable optical networks. *Sustainability, 14*(16), 10337. https://doi.org/10.3390/su141610337

Abd El-Mottaleb, S. A. A., Singh, M., Chehri, A., Ahmed, H. Y., Zeghid, M., & Khan, A. N. (2022b). Capacity enhancement for free space optics transmission system using orbital angular momentum optical code division multiple access in 5G and beyond networks. *Energies, 15*(19), 7100. https://doi.org/10.3390/en15197100

Abd El-Mottaleb, S. A. A., Singh, M., Chehri, A., Ahmed, H. Y., Zeghid, M., & Khan, A. N. (2022c). A QoS classifier based on machine learning for next-generation optical communication. *Electronics, 11*(16), 2619. https://doi.org/10.3390/electronics11162619

Abd El-Mottaleb, S. A. A., Singh, M., Chehri, A., Atieh, A., Ahmed, H. Y., & Zeghid, M. (2023). Performance of cipher image transmission in free space optics under foggy weather. *IEEE Access, 11*, 139478–139497. https://doi.org/10.1109/ACCESS.2023.3338168

Ahn, G., Jang, J., Choi, S., & Shin, D. (2024). Research on improving cyber resilience by integrating the zero trust security model with the MITRE ATT&CK matrix. *IEEE Access, 12*, 89291–89309. https://doi.org/10.1109/ACCESS.2024.3417182

Alkhamees, T. Y. A., & Milstein, L. B. (2024). Performance analysis of modern communication networks under hostile environment [Doctoral dissertation, University of California San Diego]. UC San Diego Electronic Theses and Dissertations.

Alquwayzani, A. A., & Albuali, A. A. (2024). A systematic literature review of zero trust architecture for military UAV security systems. *IEEE Access, 12*, 176033–176056. https://doi.org/10.1109/ACCESS.2024.3503587

Biswas, C., Haque, M. M., & Das Gupta, U. (2022). A modified key sifting scheme with artificial neural network based key reconciliation analysis in quantum cryptography. *IEEE Access, 10*, 72743–72757. https://doi.org/10.1109/ACCESS.2022.3188798

Cao, Y., Zhao, Y., Wang, Q., Zhang, J., Ng, S. X., & Hanzo, L. (2022). The evolution of quantum key distribution networks: On the road to the Qinternet. *IEEE Communications Surveys & Tutorials, 24*(2), 839–894. https://doi.org/10.1109/COMST.2022.3144219

Cha, S. H., Shin, M., Ham, J.-H., & Chung, M. Y. (2018). Robust mobility management scheme in tactical communication networks. *IEEE Access, 6*, 15468–15479.

Chaibi, H., Darbali, A., Quadar, N., El Rharras, A., Saadane, R., Minaoui, K., & Chehri, A. (2025). Enhancing cybersecurity through AI and blockchain: An analysis using the cybersecurity threat dataset. In M. Ben Ahmed, B. A. Abdelhakim, İ. R. Karaş, & K. Ben Ahmed (Eds.), *Innovations in smart cities applications volume 8* (Vol. 1310, pp. 525–540). Springer. https://doi.org/10.1007/978-3-031-88653-9_40

Chai, E., Shin, K. G., Lee, J., Lee, S.-J., & Etkin, R. H. (2014). Fast spectrum shaping for next-generation wireless networks. *IEEE Transactions on Mobile Computing, 13*(1), 20–34. https://doi.org/10.1109/TMC.2013.125

Chatterjee, B., Panda, P., Maity, S., Biswas, A., Roy, K., & Sen, S. (2019). Exploiting inherent error resiliency of deep neural networks to achieve extreme energy efficiency through mixed-signal neurons. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 27*(6), 1365–1377. https://doi.org/10.1109/TVLSI.2019.2896611

Chen, K., Lv, N., Zhao, S., Wang, X., & Zhao, J. (2018). A scheme for improving the communications efficiency between the control plane and data plane of the SDN-enabled airborne tactical network. *IEEE Access, 6*, 37286–37301. https://doi.org/10.1109/ACCESS.2018.2852707

Dear, V., Afero, F., Pradipta, R., Abadi, P., Arifianto, M. S., & Iskandar. (2024). Frequency window with homogeneous time of flight (ToF) for near vertical incidence skywave (NVIS) propagation determined based on ionograms. *IEEE Access, 12*, 124495–124505. https://doi.org/10.1109/ACCESS.2024.3454599

Dutta, N., & Sarma, H. K. D. (2022). Efficient mobility management in IP networks through three-layered MIPv6. *Journal of Ambient Intelligence and Humanized Computing, 13*, 3209–3227.

El Ouahmani, T., Chehri, A., & Hakem, N. (2019). Bio-inspired routing protocol in VANET networks—A case study. *Procedia Computer Science, 159*, 2384–2393. https://doi.org/10.1016/j.procs.2019.09.413

Elmasry, G. F. (2012). *Tactical wireless communications and networks: Design concepts and challenges*. Wiley.

Eswaran, S., Edwards, J., Misra, A., & Porta, T. F. L. (2012). Adaptive in-network processing for bandwidth and energy constrained mission-oriented multihop wireless networks. *IEEE Transactions on Mobile Computing, 11*(9), 1484–1498.

Fagervoll, H. M. (2017). *SDN in heterogeneous mobile tactical networks* [Master's thesis, Norwegian University of Science and Technology]. NTNU Open.

FEMA. (2018). *State and federal partners respond to the California wildfires*.

Gómez-Fragoso, J. M., Smith, M., & Santiago, M. (2022). U.S. Geological Survey response to Hurricane Maria flooding in Puerto Rico and characterization of peak streamflow observed September 20–22, 2017. *Scientific Investigations Report, 2022–5040*. U.S. Geological Survey.

Hogue, S. (2021). Project Maven, big data, and ubiquitous knowledge: The impossible promises and hidden politics of algorithmic security vision. In A. Završnik & V. Badalič (Eds.), *Automating crime prevention, surveillance, and military operations* (pp. 203–221). Springer. https://doi.org/10.1007/978-3-030-73276-9_10

INSARAG. (2023). *INSARAG after action review 2023: Türkiye and Syria earthquakes*. United Nations Office for the Coordination of Humanitarian Affairs.

Jeon, H., & Baek, H. (2024). Military non-terrestrial networks architecture and spectrum sharing method for mitigating jamming attacks and multiple access interference. *IEEE Journal on Selected Areas in Communications, 42*(5), 1465–1474.

Kamboj, P., & Pal, S. (2021). Software-defined networking in data centers. In *Software defined internet of everything* (pp. 177–203). Springer.

Kemal, L. (2023). Turkey: Inside the military's slow earthquake response. *Middle East Eye*.

Kirk, B. H., Martone, A. F., Gallagher, K. A., Narayanan, R. M., & Sherbondy, K. D. (2023). Mitigation of clutter modulation in cognitive radar for spectrum sharing applications. *IEEE Transactions on Radar Systems, 1*, 193–204.

Kumar Jagatheesaperumal, S., Rahouti, M., Chehri, A., Xiong, K., & Bieniek, J. (2025). Blockchain-based security architecture for uncrewed aerial systems in B5G/6G services and beyond: A comprehensive approach. *IEEE Open Journal of the Communications Society, 6*, 1042–1069. https://doi.org/10.1109/OJCOMS.2025.3528220

Lazrag, H., Chehri, A., Saadane, R., & Rahmani, M. D. (2019). A blockchain-based approach for optimal and secure routing in wireless sensor networks and IoT. In *2019 15th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS)* (pp. 411–415). IEEE. https://doi.org/10.1109/SITIS.2019.00072

Lazrag, H., Chehri, A., Saadane, R., & Rahmani, M. D. (2021). Efficient and secure routing protocol based on blockchain approach for wireless sensor networks. *Concurrency and Computation: Practice and Experience, 33*(11), e6144. https://doi.org/10.1002/cpe.6144

Mansoor, K., Afzal, M., Iqbal, W., Abbas, Y., Mussiraliyeva, S., & Chehri, A. (2024). PQCAIE: Post quantum cryptographic authentication scheme for IoT-based e-health systems. *Internet of Things, 27*, 101228. https://doi.org/10.1016/j.iot.2024.101228

Miao, J., Lv, N., Gao, Q., Chen, K., & Wang, X. (2022). Fault-tolerant embedding algorithm for node failure in airborne tactical network virtualization. *IEEE Access, 10*, 60558–60571.

Middlebrooks, A. J., Connell, T. G., & Vetter, R. T. (2022). The operational environment exchange network: Modeling a complex environment for resilient system design. *IEEE Transactions on Engineering Management, 69*(6), 3952–3967. https://doi.org/10.1109/TEM.2021.3123424

Mohamed, M. A., Chen, T., Su, W., & Jin, T. (2019). Proactive resilience of power systems against natural disasters: A literature review. *IEEE Access, 7*, 163778–163795.

Möhlenhof, T., Jansen, N., & Rachid, W. (2021). Reinforcement learning environment for tactical networks. In *2021 International Conference on Military Communication and Information Systems (ICMCIS)* (pp. 1–8). IEEE. https://doi.org/10.1109/ICMCIS52405.2021.9486411

Nahar, N., Andersson, K., Schelén, O., & Saguna, S. (2024). A survey on zero trust architecture: Applications and challenges of 6G networks. *IEEE Access, 12*, 94753–94764. https://doi.org/10.1109/ACCESS.2024.3425350

Niekerk, B. van. (2021). Internet of military things and information warfare. *The Air Power Journal, 1*.

Phiayura, P., & Teerakanok, S. (2023). A comprehensive framework for migrating to zero trust architecture. *IEEE Access, 11*, 19487–19511. https://doi.org/10.1109/ACCESS.2023.3248622

Quadar, A., Chehri, A., Jeon, G., Hassan, M. M., & Fortino, G. (2022)."Cybersecurity Issues of IoT in Ambient Intelligence (AmI) Environment," in *IEEE Internet of Things Magazine*, vol. 5, no. 3, pp. 140-145, September 2022, doi: 10.1109/IOTM.001.2200009.

Riaz, A., Iqbal, W., Ul Islam, F., Hassan, M., Tariq, R., Chehri, A., & Madni, A. F. (2025). S2H-securing smart homes: A blockchain-based preservation approach. *Internet of Things, 30*, 101523. https://doi.org/10.1016/j.iot.2025.101523

Ricci, S., Dobias, P., Malina, L., Hajny, J., & Jedlicka, P. (2024). Hybrid keys in practice: Combining classical, quantum and post-quantum cryptography. *IEEE Access, 12*, 23206–23219. https://doi.org/10.1109/ACCESS.2024.3364520

Saide, M. (2024). Exploring the TCP/IP protocol suite: Architecture, dominance, and future challenges in data communication. *SSRN Electronic Journal, 13*.

Sahu, S. K., & Mazumdar, K. (2024). State-of-the-art analysis of quantum cryptography: Applications and future prospects. *Frontiers in Physics, 12*, 1456491. https://doi.org/10.3389/fphy.2024.1456491

Sasada, T., Kawai, M., Masuda, Y., Taenaka, Y., & Kadobayashi, Y. (2023). Factor analysis of learning motivation difference on cybersecurity training with zero trust architecture. *IEEE Access, 11*, 141358–141374. https://doi.org/10.1109/ACCESS.2023.3341093

Suomalainen, J., Julku, J., Vehkaperä, M., & Posti, H. (2021). Securing public safety communications on commercial and tactical 5G networks: A survey and future research directions. *IEEE Open Journal of the Communications Society, 2*, 1590–1615.

Tsai, M., Lee, S., & Shieh, S. W. (2024). Strategy for implementing of zero trust architecture. *IEEE Transactions on Reliability, 73*(1), 93–100. https://doi.org/10.1109/TR.2023.3345665

U.S. Department of Defense. (2025). *Service members answer the call in California*.

Waseem, H. B., & Rana, I. A. (2025). A meta-review of disaster research. *Natural Hazards, 110*(69).

Westbrook, T. (2025). Lethal empowerment and electronic crime: A focus on radio-frequency interference capabilities. *Security and Defence Quarterly*. https://doi.org/10.35467/sdq/196515

Wu, Z., Chen, H., Lei, Y., & Xiong, H. (2020). Recognizing automatic link establishment behaviors of a short-wave radio station by an improved unidimensional DenseNet. *IEEE Access, 8*, 96055–96064. https://doi.org/10.1109/ACCESS.2020.2997380

Zeghid, M., Amaseb, K., Ahmed, H. Y., Khan, A. N., Chehri, A., & Sharma, T. (2021). Modified optical burst switching (OBS) based edge node architecture using real-time scheduling techniques. *IEEE Access, 9*, 167305–167321. https://doi.org/10.1109/ACCESS.2021.3132578

Chapter 5: The role and legal status of military intelligence in combatting hybrid threats

Eerik Heldna, ORCID: https://orcid.org/0009-0002-4686-3031

Abstract:
The imperative to "know the enemy" has been a cornerstone of military tactics for thousands of years. It is not only essential to understand the number of enemy troops, but also to assess the capabilities, intentions, and political will of hostile societies and their leaders. This knowledge is crucial for preparing military countermeasures and gathering intelligence to confront potential internal security threats—areas typically within the purview of civilian security services. For decades, democratic governance has emphasized a clear separation between military and civilian powers. In Estonia, the role of military intelligence during peacetime has been relatively constrained, particularly in the realms of counter-intelligence and security intelligence. A notable incident occurred in 2007, the so-called "spy scandal," in which Estonian military intelligence was alleged to have conducted surveillance on civilian personnel within the Ministry of Defence. Although the investigation found no wrongdoing, it underscored the constitutional significance of defining the proper role of the Estonian Defence Forces—including military intelligence—within the civilian sphere. Civilian oversight, however, does not necessarily preclude the military from collecting information on citizens and residents, especially when such activity relates to the armed forces' constitutional mandate to prepare for national defence. In the Baltic and Scandinavian regions, where conscription and reserve-based defence systems are prevalent, the interplay between civilian and military spheres is inherently more complex than in many other NATO member states. Since the deterioration of the European security environment—marked by Russia's annexation of Crimea in 2014 and the full-scale invasion of Ukraine in 2022—Estonia has gradually expanded the powers of its military intelligence apparatus. Russian military intelligence [GRU], guided by the so-called "Gerasimov Doctrine," operates in a constant state of hostility toward the "collective West," posing persistent hybrid threats. This context raises several critical questions:

- How can democratic societies balance the principle of separating military and civilian authority while effectively addressing hybrid threats?
- How can military intelligence remain both effective and legally compliant while ensuring the safety of service members at home?
- Should deeper cooperation between civilian and military intelligence agencies be pursued, or should military intelligence be granted broader authority to operate within the civilian domain?

Keywords: Military Intelligence, Estonia, Baltics, Legal Authority

Introduction

The task to "know your enemy" has been part on the military tactics for thousands of years. Sun Tzu said:

> "If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle" (Tzu, 2013).

Like information of how many troops your enemy has, to be successful on the battlefield, an army needs not only relevant piece of intel, however also the wider knowledge of what are the capabilities and intentions of the hostile society and its leaders. The knowledge is vital to prepare military counteractions and collect information to confront possible internal security threats, which usually falls into the area of responsibility of civilian security services. Therefore, should there is no doubt about the necessity to obtain relevant information- the most important question WHY is being answered, the questions WHO and HOW remain.

The clear separation between military and civilian powers has been at the core of democratic governments for decades. To a certain extent a similar sensitive question - is it acceptable for security service to have police powers beside those of traditional information collection tasks? There does not seem to be an agreed standard amongst modern democracies. The structure and tasks of different nations' security services are related to their individual historical background and traditions in this field. For example, in Germany it would not be acceptable to give policing or arrest powers to their domestic security service BfV (*Bundesamt für Verfassungschutz*). However, providing the same rights in France by DGSI (*Direction générale de la sécurité intérieure*) or Sweden by SÄPO (*Säkerhetspolisen*) do not raise the same concerns or debates (Heldna, 2016a). The author wants to underline, that similar debate was going on a decade ago in Estonia, caused by high profile anti-corruption investigations conducted by Estonian Internal Security Service. Claims have been made by some politicians during political debate, as well as in the media, that the security agencies in EU and NATO members states lack the jurisdiction to carry out procedural acts in criminal proceedings and that the law enforcement agencies do not have the right to use the information gathered by security agencies as evidence in court proceedings (Heldna, 2016b).

To sum up: The role, structure and jurisdiction of security agency powers belong wholly in the sovereign decision-making capacity of a State. In several materials analysing the field of

security of the EU it is recognised that the interpretation of the concept of national security varies greatly from State to State. The right of security agencies to carry out criminal proceedings, or the lack of it, does not contradict the principle of the rule of law (Heldna, 2016b).

The military is always preparing for the war; however, we all hope that Defence Forces will be more of an 'insurance policy' and never used in a real scenario. However, for Military Intelligence, the activities and scenarios are always for real. They do not have the luxury of purely theoretical exercises. Intelligence collected using Human Intelligence [HUMINT], Signals Intelligence [SIGINT] or other forms of intelligence, is regularly used by decision makers for the real purposes. Therefore, how much of this mixed approach used of different legal methods as described above by the example of security services, apply to Military Intelligence? We refer to the example of when a military needs to collect and process information about their civilian population during peace time and inside the State.

The role, or actually, tools, of the Military Intelligence in Estonia has been relatively limited, when it comes to the counterintelligence and security intelligence powers within the State during the peacetime. On one hand it is understandable, Military Intelligence is created to collect information about a military adversary who is typically located outside the national territory. At the same time, expectations that Military Intelligence can fulfil its key roles are getting higher: they are tasked with securing the activities of the Defence Forces domestically and providing necessary information to civilian and military decision makers. It raises questions that need to be answered:

1. How to find the balance between the legal principles of separation of the military and civilian powers, while combating hybrid threats?
2. How the Military Intelligence service can be effective and flexible following the principle of rule of law and how to keep troops safe at home?
3. Is the only answer even more close cooperation between civilian and military security services or should Military Intelligence widen the scope of activities into the civilian sector?

The author describes the topic based on the Estonian regulations and practises and his personal experience in the field of security and Military Intelligence services 2009-2020.

Legal aspects and the hybrid threats

Civilian supervision of the armed forces and a clear separation of powers does not necessarily mean total restriction to collect information. This collection could be about citizens or residents of the State. It may be related to the main task of the Defence Forces to prepare to

defend the nation by military means. However, it is one of the most sensitive questions in the democratic society.

Given there is conscript based military service in Estonia, which means a stronger reserve army system, then connection between military and civilian aspects are closer than in many other NATO member states. The worsened security situation in Europe since 2014, when Russia annexed Crimea, initiated the war in Donbass region and since 2022, when Russia started full-scale aggression against Ukraine, has caused step-by-step extension of the powers of the Military Intelligence in Estonia. Not only in the field, Russian Military Intelligence (or Russia as the regime) GRU (*Главное разведывательное управление*) is in constant stage of war with "the collective West" according to the therefore-called "Gerasimov doctrine" (Gerasimov, 2013). Even should the theory, expressed by General Valeri Gerasimov in his 2013 published article is not perhaps classical doctrine, Russian society in general, politics and military have followed these principles for a long time.

One of the distinctive features of Russian Military Intelligence compared with its counterparts in other countries is that, in addition to Military Intelligence, it also gathers information on the target countries' and regions' economy, politics, technology and ecology (Estonian Foreign Intelligence Service, 2022). Russia is obviously not a democratic state; therefore the civilian supervision, rule-of-law and other aspects of the democratic society are out question. However, the wide scope of their Military Intelligence service tasks, shows clearly that our common main adversary understands the necessity to focus on civilian targets from a military perspective. This approach gives them an advantage in the preparation stage. One of the main advantages of the Military Intelligence structures compared to the civilian security/intelligence authorities is the broader field of expertise and education. The majority of the Military Intelligence officials have two higher or professional education: one typical from the civilian branch; law, economics, political science, IT, engineering etc., and the other is a military qualification, at least at a junior staff officer level. This unique combination helps to better understand not only the broader security picture however also the adversary mind-set.

The main task of the Estonian Military Intelligence is ensuring advance warning for the military defence of the country. No doubt this is therefore to say 'pure' military task. However, collecting information necessary to achieve this goal, starts much earlier than other military actions. More than this, the preparation starts from the personnel and information security of their own troops, i.e. protection of restricted areas. Obviously, it is hard, should not impossible, to exclude civilian aspects, objects and subjects when processing the relevant and necessary data to achieve this. During the process of intelligence gathering the cooperation with civilian counterparts- security

service, police etc., play a crucial role however it is not realistic to rely on solely on partners' capacities and capabilities, especially taking into consideration the scope and specific need of the Military Intelligence. What are the hybrid security threats which we need to take closer look at from a military perspective?

Clear and complete definition of hybrid war or hybrid security threat does not exist. According to the former Commander of Estonian Military Intelligence and later Defence League, Brigade General Riho Ühtegi, hybrid war is often described through irregular war tactics (*a good example is the "little green men" in Crimea in 2014*). Irregular war tactics are an important component, however it is not the only factor in hybrid warfare (Ühtegi, 2018). Dr Frank Hoffman has said:

> "We see the convergence of military force and the interagency community, of states and nonstate actors, and of the capabilities they are armed with. What once might have been distinct operational types or categorizations among terrorism and conventional, criminal, and irregular warfare have less utility today" (Hoffman, 2009).

The definition of hybrid threats is even vaguer. It has components from hybrid warfare tactics as subversion in cyber domain, economical pressure, diplomatic means, info operations however also unexpected courses such as organized crime. Russian intelligence services have effectively utilized organized crime groups for military purposes in Crimea and strong ties exist between them. Professor Mark Galeotti has said: "The Kremlin does not control organised crime in Russia, nor is it controlled by it. Rather, organised crime prospers under Putin, because it can go with the grain of his system" (Galeotti, 2018). The term "hybrid threat" is sometimes used in conjunction with the term "asymmetric threat". An asymmetric threat can be posed by State or non-State actor e.g. recruited spy (Juht & Heldna, 2022, p. 105).

In Estonia relevant hybrid or asymmetric threats are often called internal security threats. Additionally, to the abovementioned spies, it might also be State officials having ties to organized crime, non-State actors (terrorist groups) or lack of physical or cyber security measures. These threats can change over time therefore a complete and full catalogue would be unnecessary. All of these can affect the capability of the Defence Forces by damaging personnel security. One of the main prevention tools to safeguard against these threats are background checks and a security screening process (Juht & Heldna, 2022, p. 107). Legally the countermeasures to the hybrid threats can be divided into two major categories:

1. Law enforcement reactive measures (*typically criminal proceedings*) when the threat materializes (*when an offence has been committed*). In some cases,

military police can exercise those countermeasures, however in most cases, it is the responsibility of the civilian law enforcement bodies.

2. Preventive measures, e.g abovementioned security screening however also general policymaking, regulations which supports processes etc.

Estonian Security Authorities

There are two designated security authorities and one specialized intelligence unit within the Estonian Defence Forces [EDF], responsible for carrying out intelligence activities. However, two of them: Estonian Foreign Intelligence Service [EFIS] and Estonian Internal Security Service [ISS] are operating according the Security Authorities Act (*julgeolekuasutuste seadus*, the abbreviation in Estonian is [JAS]). The Estonian Military Intelligence Centre [EMIC] is operating based on the tasks stipulated in the fourth chapter of the Defence Forces Organisation Act (*kaitseväe korralduse seadus*, [KKS]). From the legal perspective EMIC is not a security authority, however the functions and even supervision, conducted by the relevant Parliamentary Committee, is almost the same. The author will not focus much on the functions of EFIS or ISS, only to explain the differences of legal means when it comes to fulfil the tasks stipulated in the relevant legal acts. Due to the ISS having a dual role- policing in the field of high-level corruption and terrorism crimes which is obviously out of the scope of EFIS and EMIC, the author will not compare those tasks and relevant police powers (*e.g. house search, arrest etc*.) which are outside the scope of intelligence/counterintelligence activities. Police powers of the ISS are stipulated in JAS § 21.

The basic division between those services is simple- ISS operates within Estonia, EFIS, outside our borders. ISS is under the Ministry of Interior and EFIS is under the Ministry of Defence [MoD]. EMIC as a part of the EDF is obviously subordinated (*via EDF*) to the MoD. Among the other tasks, ISS is tasked for:

1. Preserving constitutional order and territorial integrity,
2. Prevention and combating of intelligence activities directed against the State. This includes protection of State secrets and classified information of foreign states in the cases and according to the rules prescribed in the State Secrets and Classified Information of Foreign States Act (*counterintelligence*).

The primary task of the EFIS is collection and processing of information about foreign states, or foreign activities which is relevant for the State in formulating the foreign, economic and national defence policy and for national defence. Both, EFIS and ISS can use the same following methods stipulated in JAS:

- examination of a postal item;

- wiretapping, observing or recording a message or other information transmitted over an electronic communication network;
- wiretapping, observing or recording information communicated by any other means
- recruitment of person to secret co-operation
- use of legal person in private law
- appoint on a post or recruit an undercover staff official or employee of the security authority
- collection and processing of personal data;
- covert surveillance;
- covert establishment of identity;
- collection of information on the fact, duration, manner and form of transmission of messages over an electronic communications network and on the personal data and location of the sender or receiver of such messages;
- covert entry in the person's premises, building, enclosed area, vehicle or computer system for the purposes of covert collection or recording of information or installation and removal of technical aids necessary for such purposes;
- covert examination of an item and, should necessary, covert alteration of the item, damage to the item or replacement of the item.

The Head of Tallinn Administrative Court or a judge appointed by him/her, is responsible for the authorisation of the abovementioned methods. For some less intrusive methods, the authorisation of the Head of Service is needed. The author states that the abovementioned methods support the activities of the ISS and EFIS. However, when it comes to operational activities outside of the Estonian borders, this court approval is somewhat a formality- the covert collection of data carried out in a territory foreign would likely be criminal act in that territory.

Development of the Estonian Military Intelligence Centre (EMIC)

Before the World War II, Estonia had two security services. Political police (*PolPol- poliitiline politsei*) was the predecessor of the modern ISS. The original name was (*and it is today in Estonian*) Security Police- [KAPO] (*Kaitsepolitseiamet*). It has its roots in the War of Independence (1918-1920), when Information Collection Department (*teadete kogumise jaoskond*) was created within Operational Department of Defence Forces (Juurvee, 2018, p. 26). Staff of this unit was transferred to the newly established KAPO in begging of 1920 (Juurvee, 2018, p. 41).

The predecessor of the EMIC was the other branch of Defence Forces- Reconnaissance Department (*maakuulamise jaoskond*), which mainly conducted collecting and processing intelligence information from the tactical level however also interrogation of prisoners of war (Juurvee, 2018, p. 27). In spring 1920, after the victory in the War on Independence, reorganisation followed and in 1924 Military Intelligence obtained the structure which existed until 1940- II Department (Juurvee, 2018, p. 44). Therefore, both services, the civilian and later part of the police and the military one, have origin from the military forces. The Soviet and Nazi occupations stopped the development, and it could continue only 50 years later.

The need to collect and process intelligence was clear since the re-establishing of the EDF in 1992. The hardest question was, how to organize the data collection and where should be the focus? Of course, capabilities and capacity were the key issues. Some sort of SIGINT started in 1994 (Juurvee, 2018, p. 160). In the begging the function of the Military Intelligence was designated to the Second Department of the EDF HQ- J2. J2 grow and developed, like the other sister agencies: EFIS (Information Board until 2017) and KAPO, legal regulations were not complete. perhaps it is not the best comparison however the Intelligence Services Act, which finally established Secret Intelligence Service (SIS, MI6) was adopted in 1994 (Intelligence Service Act, 1994).

The significant change for Military Intelligence took place 13 March 1998 when the Military Intelligence Battalion of Estonian Defence Forces was created. This date is celebrated as the birthday of the Estonian Military Intelligence. Since May 2013 the unit was placed under the direct command of the Commander of the EDF. The name of the battalion did not reflect the real character of the unit- it was not a tactical level unit, what a battalion is, rather than specific command. The evaluation continued and since 2014 it was re-organized and renamed Estonian Military Intelligence Centre [EMIC].

What did not follow with the same pace and created several problems later, were necessary legal amendments. In 2000, Security Authorities Act were adopted and the ISS and EFIS obtained clear legal operational ground. Military Intelligence was left out it and continued to operate on vague grounds. The supervision was delegated to the MoD and Riigikogu, like EFIS and ISS however it did not solve somewhat a legal vacuum.

The “spy scandal” of 2007 and later legal developments

In 2007, the so-called “spy scandal” took place in Estonia. Estonian Military Intelligence during 2005-2006 allegedly collected counter-intelligence information about the civilian staff of the Ministry of Defence of Estonia (Vahter & Velder, 2007). The “counterintelligence information” was

actually only a few reports (no wiretapping, covert entry etc), describing contacts and behaviour of some officials of MoD. A criminal case was opened, and the investigation was conducted by the ISS under the guidance of the General Prosecutor's Office. Initially, Military Intelligence was publicly accused violating the law, however already then, some signs of unhealthy rivalry were noticed- even Minister of Interior, formed head of ISS, stated that Military Intelligence is moving towards the goal to become the third security authority (Roonemaa, 2008). Political tensions were high, even today, some political decisions which followed, e.g. reducing the rights of Military Intelligence, are called emotionally as "the murder of Military Intelligence" (Roosimägi, 2009). The criminal investigation found no guilt of concrete persons and was closed. However, the Commander of Military Intelligence Battalion- predecessor of EMIC, was transferred to another position, some other high-level officials of EDF HQ left their positions. This event raised the question about the role of the Estonian Defence Forces [EDF] operating in the civilian environment, inter alia in the field of Military Intelligence. It is important to mention that during this period Military Intelligence was regularly supervised both by the MoD and the parliamentary committee, which was one of the grounds to terminate the further investigation (Vahter & Ideon, 2008). Remarkable that the Chancellor of Justice who also analysed this incident, stressed- the Government and the Parliament [*Riigikogu*] are responsible for the situation where tasks and legal tools are out of balance and not stipulated in law (*Õiguskantsler*, n.d.).

The first political reaction was to deprive Military Intelligence of major part of the operational rights within Estonia. EDF HQ lost its status as the criminal intelligence authority in 2009 (Jälitustegevuse seadus, n.d.). Military Police [MP] replaced this function, however the tasks of the MP were totally different and had more law enforcement than intelligence approach. Until 2009, J2 was conducting security vetting of all EDF personnel and military personnel assigned to the MoD. Protection of classified information is an essential part of counterintelligence and security vetting is part of it. should EFIS and ISS continued with this practise, EMIC lost this function however the task to protect the classified information remained. Obviously, it became like boxing with one hand. Additionally, it had strong negative impact for the working moral, mistrust towards J2 staff did not bring anything good. Gradually, especially after the Russian aggression started in Crimea and Donbass, the necessity to empower Military Intelligence became clearer. What does not mean that legal framework did the same. Vice versa, because relevant legislation was adjusted step-by-step, it caused some contradictory regulations, which will be presented below.

In 2008 the first regulations for Military Intelligence appeared in the KKS and several significant amendments followed in 2012, 2014 and 2016. However, it did not solve the core issue of the Military Intelligence- the clear position in the security authorities' hierarchy. Unfortunately,

despite the improvement since then, especially after 2019-20, the tasks and legal tools are still not aligned to the full extent of necessity. One of the major positive improvements has been the amendment, entered into force 10 January 2023, which stipulated that besides collecting and processing the information for the Military Intelligence purposes, the same methods to collect information is allowed in order to conduct, prepare and organize armed resistance. Taking into consideration the Russian aggression in Ukraine, this is a highly welcomed amendment.

It did not go smoothly though. In 2018 the first attempt to systematically empower EMIC was made. The new version of the intelligence chapter in KKS was drafted and it was passed to Riigikogu in February 2019. One of the main amendments was the possibility to conduct intelligence activities in order to guarantee security of the restricted areas on the territory of Estonia and during the peacetime. However surprisingly, the President of the Republic refused to proclaim the law. There were two main arguments: one was that Defence Forces will have too broad area of activities in the peace time, according to the President it should be narrowed and focused on military activities. The interpretation of the President was that Constitution forbids wider role of Defence Forces in peace time, especially when it comes to the data collection which is inevitable while securing the restricted areas. The second reason was that more detailed and focused on the problem that the supervision, how civilians would be informed that their personal data has been processed, was not clear (Riigikohus, 2019). Minister of Justice, Minister of Defence, Riigikogu and Chancellor of Justice disagreed (Riigikohus, 2019). According to the Constitution, Riigikogu passed it a second time without changes and President went to the Supreme Court. The decision of 19 December 2019, put important benchmarks for the future. It was interesting that during the written hearing Minister of Interior stated that should the legal analysis and later legislation clearly divides the responsibilities of services, he supports passing the law. ISS, however, supported the claim of the President, stating that passing the law gives EMIC similar powers as to the security service (Riigikohus, 2019). Supreme Court agreed with the President that the law contradicts the Constitution however only because the supervision of the intelligence activities is not stipulated to meet the necessary requirements (Riigikohus, 2019). However the Supreme Court stressed some important fundamental principles concerning the role of Defence Forces combatting internal security threats during the peacetime within the State. Due to the nature of Defence Forces, which is special compared to the rest of the executive branch, the Constitution set limits however does not totally forbid to give Defence Forces authority to conduct covert surveillance or colleting and processing data during the peacetime should this activity is related to fulfil the main tasks. It is not forbidden that Defence Forces exercise the law enforcement functions should it is clearly stipulated in law and civil supervision is applied (Riigikohus, 2019).

The amendments concerning more detailed supervision were added and the law came into force 5 June 2020. Beside the legal developments, structural changes were made in order to strengthen the EMIC capability to counter the internal security threats. Additionally, to the position of Deputy Commander of EMIC in the field of intelligence the position of Deputy Commander in the field of security was established, (*author held this position 2018-2020*).

Current tasks of the EMIC

KKS is the sole legal act which gives the definition of the intelligence or to be precise, Military Intelligence (*article 36 of the fourth chapter*) (*Kaitseväe korralduse seadus*, n.d.):

(1) Military Intelligence is collecting and processing information by the Defence Forces:

1) for military defence of the State;

2) for preparation and conduct of international military operation;

3) for the prevention of and combating intelligence activities directed against the State in the cases and pursuant to the procedure prescribed in the State Secrets and Classified Information of Foreign States Act;

4) for the defence of a military unit of the Defence Forces participating in an operation in the area of an international military operation pursuant to the procedure prescribed in this Act;

5) for the conduct of background check;

6) for the protection of the restricted military area of the Defence Forces.

The tasks of EMIC are stipulated in detail in the Statue of the Defence Forces (*Kaitseväe põhimäärus*, n.d.).

1. ensure advance warning for the military defence of the country;
2. perform defence intelligence and coordinate the intelligence and security activities of other structural units;
3. provide intelligence and security information to the Ministry of Defence, the Chief of the Defence Forces and the Deputy Chief of the Defence Forces;
4. perform a background check when assessing the suitability of a person applying for service or work in the Defence Forces, as well as an active-duty soldier, official or employee, and when deciding whether to admit persons related to the provision of services to the Defence Forces into the security area of the Defence Forces;
5. organize the protection of State secrets in the Defence Forces;

6. supervision of the fulfilment of the requirements of the State Secrets and Classified Foreign Information Act and the legislation issued on the basis thereof in the Defence Forces and the Defence League

Among the six tasks set out in KKS Article 36, several fall clearly within the realm of hybrid or internal security threats. These include the prevention and combating of intelligence activities directed against the state, carried out in accordance with the State Secrets and Classified Information of Foreign States Act; the conduct of background checks to ensure the reliability and integrity of individuals in sensitive positions; and the protection of restricted military areas belonging to the Defence Forces. Together, these tasks illustrate the state's responsibility not only to defend against external threats but also to safeguard its institutional resilience and internal security environment.

Although these tasks are broad, the legal means available to EMIC to implement them remain comparatively limited when set against the authorities of the ISS or EFIS described above. EMIC is authorised to collect and process signals transmitted outside public communications networks located within Estonian territory; imagery of the earth, sea, or objects used by a foreign state that are situated outside Estonia or that have entered its territory; unrestricted information from other holders as well as restricted information obtained under the Public Information Act or the State Secrets and Classified Information of Foreign States Act; and information gathered under §39, meaning that EMIC may request professional assistance from EFIS for collecting information necessary for the military defence of the state, though not for EMIC's other statutory tasks such as the protection of restricted military areas. In addition, EMIC may process information obtained from public sources by any other lawful means, effectively encompassing open-source intelligence. EMIC additionally may involve a person in secret cooperation. Not for protection of the restricted area, however to simulate a legal person governed by private law, a structural unit, body thereof, or a branch of a company as use as an undercover agent in order to act outside of the territory of the Republic of Estonia; to interview persons, involve a person in secret cooperation, use shadow information and conspiracy techniques, when already outside of the territory (*e.g in a military operation area*), conducting covert intelligence (*surveillance*) is allowed.

Instead of going by the simplest way- adding EMIC to listed security authorities (JAS § 7), somewhat a LEGO building strategy was chosen, adding new roles piece by piece. The proposal to make amendment to JAS, was presented several times in recent years, the last time in Estonian Riigikogu this year. The necessity is clear and during the discussions in Riigikogu the Commander of EMIC was invited and expressed his opinion- this amendment is much needed (Riigikogu, 2024).

However, supported by 41 votes, 3 against and 0 abstained, the debates of the legal draft were cancelled for this time (Riigikogu, 2024).

It is hard to find the clear explanation why the legislative branch has decided to gradually change or add some new do therefore, however author states, based on his personal professional experience and protocols of the discussions in Riigikogu (Riigkogu, 2018), that behind it, one can find a reluctance to create a third security service, possibly due to the fear that it will create somewhat rivalry when it comes counterintelligence activities. This reluctance has been expressed by some decision makers, during the discussions in media and in Riigikogu.

Some examples of confusing regulations. According to the KKS article 36, EMIC bears the responsibility for the defence of a military unit of the Defence Forces participating in an operation in the area of an international military operation. This task allows to covertly collect and process information and conduct covert surveillance and collect SIGINT. should, for example, information obtained that group of individuals are planning to conduct an attack against Estonian troops position in Iraq, EMIC is authorised to listen to their radio communications, conduct covert surveillance, however, not listen and record their conversation onsite. At the same time, EFIS, who is responsible for counterintelligence to protect EDF troops stationed outside Estonia, can do it, should it is necessary to prevent hostile intelligence. Therefore, should instead of terrorists planning to attack the base, someone plans to recruit Estonian officer then eavesdropping is allowed however not to prevent terrorist act. Of course, theoretically cooperation between the services would help to resolve this scenario, however author has opinion that such complicated wordings even for the persons with legal education, not supporting the legal clarity principle.

One of the most sensitive topics for any intelligence service, is the human source. EMIC has legal right to involve a person in a secret cooperation. In certain cases, it is urgently needed to control the suitability of this person. KKS § 37 stipulates *expressis verbis* that this cooperation with the Defence Forces is not known to third persons. KKS allows EMIC to use covert surveillance for this purpose. However, when EMIC decides to use this method then KKS § 37 (4^4) applies which stipulates that EDF. […] shall notify the Estonian Internal Security Service immediately of the decision to use covert surveillance". This requirement does not apply neither to EFIS or ISS. The problem is not the theoretical distrust between the services; however, this is the question of need-to-know principle. Obviously, informing the third party, even the trustworthy one, violates this principle.

After the security vetting task was transferred to the ISS in 2009, conducting of background check remained the task of the EMIC. Not all positions in the EDF requires access to State secrets above CONFIDENTIAL level. However, conducting of regular background check applies to all the

staff of EDF, Military Academy, in some cases to the reservists, when they are appointed to the war time positions. It means thousands of people and also civilian private counterparts who provides different services to the EDF. According to the KKS § 415, while conducting the background check it is allowed to use following intrusive intelligence methods:

1) recruit a person in secret cooperation; for example, a neighbour to receive background information about the EDF employee;
2) use shadow information and conspiracy techniques; for example, questioning someone hiding the real identity of EMIC officers;
3) conduct covert surveillance of a person.

These methods are intrusive and sensitive. At the same time much less intrusive method, like an enquiry to the communications, basically to identify the people who communicate with the EDF employee, is forbidden. Surprisingly, according KKS § 42^2 it is allowed should the EDF employee works at the MP, however not should she or he works at the Special Operations. Of course, via the security vetting conducted by the ISS, necessary information will be processed however according to authors´ opinion it shows lack of more systematic approach. It is highly unlikely that abovementioned examples were the lawmaker's intention rather than result of constant adjustments of regulations instead of complete revision of legal regulations.

The status of the intelligence services in neighbouring countries

Latvia

There are three intelligence/security services in Latvia, Constitution Protection Bureau (*Satversmes aizsardzības birojs*, [SAB]), who has in general civilian intelligence function, Latvian State Security Service (*Valsts drošības dienests*, [VDD]) and Latvian Defence Intelligence and Security Service, (*Militārās izlūkošanas un drošības dienests, saīsināti*, [MIDD]). Like EFIS in Estonia, as the National Security Authority, SAB also ensures protection of NATO and EU classified information in public institutions engaged in work with such information (State Security Service of Latvia, n.d.). According to the Law on State Security Institutions, section 14 (Law on State Security Institutions), MIDD, is one of the three security institutions of Latvia. The MIDD is tasked to:

1. Obtain and provide the Ministry of Defence, its subordinate institutions and other government bodies and their responsible officials, as well as the National Armed Forces with intelligence and counterintelligence information necessary for their operation.
2. Detect and in cooperation with other State security institutions prevent subversive activities of foreign special services, organisations and individuals

within the Ministry of Defence, its subordinate institutions, and the National Armed Forces.

3. Take measures to protect official secrets within the Ministry of Defence, its subordinate institutions, and the National Armed Forces, as well as control the implementation of such measures.
4. Vet the candidates willing to obtain special permits (licences) issued by the Ministry of Defence to carry out certain types of commercial activity that is subject to licencing and provide an opinion on the issuance of special permits (licences).
5. As the national institution for signals intelligence, carry out and control signals intelligence and ensure the protection of the obtained information.
6. Be the subject of investigatory operations within the scope of its competence.
7. Fulfil other tasks as defined by laws and regulations and international agreements, including in ensuring effective information exchange with NATO and EU bodies and partner countries.

Lithuania

Lithuania has two intelligence/security services, one civilian (*Valstybės saugumo departamentas* [VSD]), and Military Intelligence, both can use the same methods in their area of expertise. Lithuania has decided to separate police powers from VSD, not like in Estonia or Latvia, where security services have the police powers while conducting investigations in their field of responsibility. Under the law of December 23, 2010, the pre-trial investigation function of VSD was eliminated. It was the expression of political will to treat the Department as the intelligence institution and not as the legal enforcement one. Activities of VSD were adjusted and intelligence and counterintelligence, as the main fields of activities of the institution have been developed purposefully (*Lietuvos Respublikos valstybės saugumo departamentas*, 1990). Behind this decision and VSD reform in general, was not only the pure legal analysis. Like in Estonia “spy scandal” played its role. The VSD involvement in CIA secret prisons program (ICDS, 2010), when 8 persons were detained at the secret prison near Vilnius, ended up in the court hearings in the ECHR (ECHR, 2018). Obviously, the situation raised the questions about the role of VSD, the reform followed, which did lead to the currently valid legal framework.

The Second Investigation Department under the Ministry of National Defence (*Antrasis operatyviniu tarnybu departamentas* [AOTD]) is directly responsible to and tasked by the Minister of National Defence. AOTD is responsible for conducting intelligence and counterintelligence in

the areas of defence, politico-military, military-economic, military-technical and military information. It is also responsible for the information security within the National Defence System and its diplomatic institutions (AOTD, n.d.). The tasks of the AOTD are stipulated in Law of Intelligence, Section 3, Article 8: (Republic of Lithuania Law on Intelligence)

> 3. The Second Investigation Department shall carry out intelligence and counter-intelligence activities in the following areas:
>
> 1) defence, military-political, military-economic, military-technological and military-information areas;
> 2) activities of institutions of the national defence system of the Republic of Lithuania abroad;
> 3) protection of information comprising a State secret and an official secret of institutions of the national defence system of the Republic of Lithuania.

Finland

There is similar system in Finland as in Lithuania. Finland has two intelligence/security services: domestic SUPO within the Ministry of Interior (*origins as the police branch*) and Military Intelligence- Finnish Defence Intelligence Agency (*Puolustusvoimien tiedustelulaitos*, [FDIA]) within the Ministry of Defence. It was formed on 1 May 2014 by merging the Finnish Military Intelligence Centre, the Finnish Intelligence Research Establishment and counter-intelligence assets from the Intelligence Division. In addition to the FDIA, the Act on Military Intelligence, Section 11, stipulates the Defence Command of the Finnish Defence Forces as the Military Intelligence authority, while carrying out Military Intelligence activities (Acts on Military Intelligence, 2019). The tasks of the Finnish Military Intelligence are stipulated in Section 4, Military Intelligence is targeted at the following activities should they are of a military nature:

1) activities by a foreign country's armed forces and organised troops comparable to them, and preparing such activities;
2) intelligence activities targeting Finland's national defence;
3) design, manufacture, distribution and use of weapons of mass destruction;
4) development and distribution of military supplies of a foreign country;
5) a crisis that poses a serious threat to international peace and security;
6) activities that pose a serious threat to the security of international crisis management operations;
7) activities that pose a serious threat to safety when Finland provides international

assistance or is involved in other international activities.

In addition, Military Intelligence is targeted at activities by a foreign country or other activities that pose a serious threat to Finland's national defence or endanger functions vital to society (Acts on Military Intelligence, 2019).

Conclusion

There are three institutions who are working to guarantee the security of the State in Estonia. One of them is a part of EDF, therefore the question of civilian supervision has always been in the air.

Without any doubt Defence Forces are special branch of the executive branch. Separation of powers, together with civilian control principle requires that all the powers, given to the military, especially in the peacetime, have to be considered carefully by legislative branch and subordinated to the strict judicial control. However, it must not stop the Defence Forces to obtain necessary information, which is vital for military defence of the State, however at the same time supports the requirements of physical, operational, informational security of the Defence Forces. The decision of the Supreme Court of Estonia, 19 December 2019, presented clearly- those goals are not contradictory or against the rule-of-law or other fundamental principles of democratic society and it is the question of political will, how the Military Intelligence is organized.

Based on the experience and legal analysis, author expresses his opinion that the legal regulation of the EMIC activities is not supporting its goals to the full extend. The current security situation, hybrid threats and changed approach to the military areas of expertise requires simple, clear and concise regulation, which according to the author is achievable by adding EMIC as one of the three security authorities and finally giving EMIC the necessary formal legal status.

The main difference with the EMIC is that MIDD, AOTD and FDIA are all clearly mentioned as the security or intelligence authorities. From the legal perspective this supports legal clarity- tasks, responsibilities and legal boundaries of the similar State institutions are easily found in one legal document. In authors 'opinion, Estonia should follow the neighbours' path and stipulate the tasks of internal security, foreign intelligence and Military Intelligence according to the same principles. Currently there is much space for improvement.

References

European Court of Human Rights. (2018). *Al-Hawsawi v. Lithuania* (Application no. 36998/14). https://hudoc.echr.coe.int/app/conversion/pdf/?filename=Judgment+al-Hawsawi+v.+Lithuania+-+complicity+in+CIA+secret+detainee+programme%2C+multiple+violations.pdf&id=003-7850027-10902978&library=ECHR

Estonian Foreign Intelligence Service. (2022). *International security and Estonia*. https://raport.valisluureamet.ee/2022/en/russian-armed-forces/gru-intelligence-centres/

Finlex. (2019). *Act on Military Intelligence* (No. 590/2019). https://www.finlex.fi/sv/laki/kaannokset/2019/en20190590.pdf

Galeotti, M. (2014, March 7). Commentary: Crime and Crimea — Criminals as allies and agents. *Radio Free Europe/Radio Liberty*. https://www.rferl.org/a/crimea-crime-criminals-as-agents-allies/26671923.html

Galeotti, M. (2018, March 23). *Gangster's paradise: How organised crime took over Russia*. *The Guardian*. https://www.theguardian.com/news/2018/mar/23/how-organised-crime-took-over-russia-vory-super-mafia

Heldna, E. (2016a). *Julgeolekuasutuste kogutud informatsiooni kasutamine kriminaalmenetluses ja jagamine uurimisasutustega*. *Juridica X*.

Heldna, E. (2016b). *Use of information collected by security agencies in criminal proceedings and sharing it with law enforcement agencies* [Summary of master's thesis, University of Tartu]. https://dspace.ut.ee/server/api/core/bitstreams/cb73525f-5bb1-48d7-be9e-8324b880947e/content

Hoffman, F. G. (2009). *Hybrid warfare and challenges*. *Joint Force Quarterly*, (52), 34–39. https://smallwarsjournal.com/documents/jfqhoffman.pdf

Intelligence Services Act 1994, c. 13. https://www.legislation.gov.uk/ukpga/1994/13/contents

Juht, S.-A., & Heldna, E. (2022). *Kaitseväeluure riigisisese julgeolekumeetmed*. *Turvalisuskompass*, (3), 105. https://digiriiul.sisekaitse.ee/bitstream/handle/123456789/3173/kaitsev%c3%a4eluure%20riigisisese%20julgeoelku%20meetmed.pdf?sequence=1&isAllowed=y

Juurvee, I. (2018). *100 aastat luuret ja vastuluuret Eestis*. *Post Factum*. https://www.riigikohus.ee/sites/default/files/elfinder/dokumendid/et/100_aastat_luuret_ja_vastuluuret_eestis.pdf

Kaitseväe korralduse seadus, RT I 2022, 14, § 36. https://www.riigiteataja.ee/akt/121062024014#para36

Kaitseväe põhimäärus, RT I 2023, 13, § 13. https://www.riigiteataja.ee/akt/128062023013#para13

Lietuvos Respublikos valstybės saugumo departamentas. (n.d.). *Development of the State Security Department from 1990*. https://www.vsd.lt/en/activities/history/development-of-the-state-security-department-from-1990/development-of-the-state-security-department-from-1990/

Lithuanian Ministry of National Defence. (n.d.). *Second Investigation Department*. https://kam.lt/en/antrasis-operatyviniu-tarnybu-departamentas/

Seimas of the Republic of Lithuania. (2022). *Law on Intelligence*. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/5b8dadd0f22b11ecbfe9c72e552dd5bd

Saeima. (1995). *Law on State Security Institutions*. https://likumi.lv/ta/en/en/id/57256-on-state-security-institutions

Riigikohus. (2019). *Lahend nr 5-19-38/15*. https://www.riigikohus.ee/et/lahendid?asjaNr=5-19-38/15

Riigikogu. (2023). *JAS § 21*. https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/524032023002/consolide#para21

Riigikogu. (2024, May 8). *Päevakorra nr 14 protokoll*. https://stenogrammid.riigikogu.ee/et/202405081400?phrase=kaitsev%C3%A4eluure&type=ALL#PKP-839095

Riigikogu. (n.d.). *List of the protocols of the Riigikogu debates about the tasks of the military intelligence*. https://stenogrammid.riigikogu.ee/et?rangeFrom=01.05.2018&rangeTo=&singleDate=&phrase=kaitsev%C3%A4eluure&type=ALL

Roonemaa, H. (2008, March 14). *Sõjaväeluure ülem: Ilvese järele pole nuhitud! Delfi*. https://www.delfi.ee/artikkel/19143724/sojavaeluure-ulem-ilvese-jarele-pole-nuhitud
Roosimägi, U. (2009, January 19). *Urmas Roosimägi: Sõnumitooja tapmine – Eesti sõjaväeluure saatus*. *Postimees*. https://arvamus.postimees.ee/171328/urmas-roosimagi-sonumitooja-tapmine-eesti-sojavaeluure-saatus
Sun Tzu. (2013). *The art of war* (T. Cleary, Trans.). Shambhala.
Ühtegi, R. (2018). *Venemaa hübriidsõda Georgias 2008*. *Sõjateadlane*, (7), 63. https://www.kvak.ee/files/2019/02/sojateadlane_7_www.pdf
Vahter, T., & Ideon, A. (2008, May 28). *Sõjaväeluurajatele halastati*. *Ekspress*. https://web.archive.org/web/20120824033037/http://www.ekspress.ee/news/paevauudised/eestiuudised/sojavaeluurajatele-halastati.d?id=27676449
Vahter, T., & Vedler, S. (2007, February 22). *Sõjaväeluure nuhkis riigiametnike järele*. *Ekspress*. https://ekspress.delfi.ee/artikkel/69093529/sojavaeluure-nuhkis-riigiametnike-jarele
Õiguskantsler. (n.d.). *Kaitseväes toimuva eest vastutavad Vabariigi Valitsus, Kaitseministeerium ja Kaitsejõudude Peastaap*. *Õiguskantsler*. https://www.oiguskantsler.ee/et/%C3%B5iguskantsler-kaitsev%C3%A4es-toimuva-eest-vastutavad-vabariigi-valitsus-kaitseministeerium-ja
Jälitustegevuse seadus, RT I 1996, 55, 1050. https://www.riigiteataja.ee/akt/13003193

Section 2: Modernization of Military Capabilities

Chapter 6: Forming an Analytic Framework for the Communication of the Military Utility of Technology

Lt-Col./Dr Kent **Andersson**, ORCID: https://orcid.org/0000-0001-6104-5788
Lt-Col./Dr Patrik **Stensson**

"Technological change of relevance to military innovation may be faster and more consequential in the next 20 years than it has proven to be over the last 20." (O´Hanlon, 2020)

Abstract:

Against the backdrop of a deteriorating security situation in Europe, there is an increased need for research and technology activities (R&D) to support the development of military capabilities. This case study focuses on Sweden. The Swedish Armed Forces' R&D budget is planned to increase in the coming period. At the same time, the Swedish Armed Forces have decided to review the process of their knowledge development. In an increasingly complex world with a society development that is becoming more and more difficult to predict, the importance of understanding how research funds can be best utilized also increases. This is an initial report in a study aimed at contributing to improved communication regarding technical forecasting within military capability development. Assumptions about seven central theoretical and conceptual starting points for the dialogue between consumers and producers of technical forecasts will be discussed. From these, a number of interests formulated as questions have been derived. A compilation of these questions is presented as a preliminary proposal for a framework for analysis. The framework is expected to evolve based on lessons learned in a continued study where the framework is to be applied in assessments commissioned by the Swedish Armed Forces.

Keywords: Communications Technology, Research and Development

Introduction

Extensive efforts within science and technology [S&T] are crucial for armed forces to maintain relevance of military capabilities over time. After a period of decline in Swedish S&T-spending since the end of the cold war, there is now a sense of urgency. For example, a defence innovation initiative launched in 2023 by the Swedish government aimed at increasing the capacity and pace of innovation in the Swedish defence sector (Government offices of Sweden, n.d.). Furthermore, the Swedish government acknowledges in a new strategic direction for defence innovation the need to accelerate and mutually strengthen innovation in the military and civilian sectors (Ministry of Defence [MoD], 2024). Since the low point in 2017, the Swedish Armed Forces' S&T budget is now planned to be tripled or quadrupled by 2030. In an increasingly complex world

with an ever more unpredictable societal development, we argue the importance of also increasing the understanding of how research funds are used most effectively (Swedish Armed Forces, 2021b). This is especially true for technological development, where advancements in areas such as cyber and artificial intelligence affect both the continued digitalisation of society and the development within diverse technological sciences. For a long time, most technical innovations have taken place in the civilian sector. Here, the activity labelled Technical Forecast has long been responsible for knowledge development aimed at providing the Swedish Armed Forces' studies and concept development with insights and forecasts regarding technological developments in society. However, the S&T activities, including a program for Horizon Scanning and the Technical Forecasting, have undergone major changes due to earlier cutbacks and are now in a rebuilding phase. No doubt the situation is similar in other parts of NATO. This phase does not aim to return to the previous form but to evolve into something that better suits the Swedish Armed Forces of the new era. This is described in the S&T directive document for 2022-2025, IFoU 22-25 (Swedish Armed Forces, 2021b).

Since the mid-00s, there has been an ongoing transformation from threat-based to capability-based planning and development in the Western world. This shift changes the perspective on technological development from being platform-centered to a more capability-centered view (US Department of Defense, 2008). It entails a systems view of capability where a defence force cannot afford to sub-optimize the technical components (Fitzsimmons, 2007). Instead, as indicated by Andersson (2020), these components should be evaluated as system elements in interaction with social components, such as doctrine, organization, and training, in order to achieve the desired effects.

A benefit of the current process for technical forecasting, in a changing environment with an increasingly rapid pace of technological development, is its flexibility with relatively short turnaround times from identifying interesting technology areas to assessing their development (Silfverskiöld et al., 2021). However, this might come at the expense of a comprehensive view and depth in the analyses. To mitigate this risk, and to support a capability-centred view of technological development, the method for technical forecasting in Sweden was supplemented about 10 years ago with an in-depth assessment of the studied technologies' military utility (Andersson et al., 2019). The outcome of such an assessment determines whether the future technology in question can be considered to have significant, moderate, negligible, or uncertain military utility for the Swedish Armed Forces. It also includes a recommendation on how to continue the knowledge development regarding the technology - to actively participate in an appropriate

form or to refrain. If the technology is assessed as having moderate or uncertain utility, the usual recommendation is to monitor the development and renew the assessment within a few years.

A report from a study on the validity of the method for assessing the military utility of future technologies (Silfverskiöld et al., 2021) revealed several shortcomings and limitations. The most central remaining question is how the assessment of military utility meets decision-makers' needs for supporting data in the capability development process. Is this crucial for determining which technologies are deemed important to consider? The report highlights several aspects that reasonably affect how much weight an information recipient should place on the assessment:

- It does not clearly consider how composite the technologies are, i.e., whether they are fundamental and part of many applications or if they combine other technologies into a specific function.
- It only indirectly includes an assessment of utility relative to competing technologies, and the selection of technologies risks highlighting some while concealing other potentially important technological developments.
- It is made against capabilities in the Armed Forces' capability portfolio that have significant impact, without explicit directions to potentially prioritized tasks and capabilities.
- It is made against the backdrop of a prediction of the capability in focus, taking into account a range of related societal change drivers, not just technological development, but the uncertainties in the analysis of these vary greatly and are not reflected in the aggregated result.

The input to the assessment of military utility consists of forecasts concerning the development of the technology in focus. These are authored by various research institutes, such as the Fraunhofer Institute for Technological Trend Analysis, and usually contain an overview of the technology in focus, its potential advantages and disadvantages, possible applications, which actors show the most interest, the development of sub-technologies, and a timeline for when the technology will become operational. Reports on hypersonic propulsion (Nätzker & Huppertz, 2017) and on cognitive radar (Karsten, 2018) serve as examples to this study and can be obtained upon request.

The importance of determining and demonstrating the potential military relevance of technological innovation as soon as possible was highlighted in a research study by Modig and Andersson (2021). The study shows that only when the technology is perceived as militarily relevant by the collective that makes decisions in capability development is it likely to lead to

military innovation. Failure to demonstrate military relevance risks leading to delays, missed opportunities, and, in the worst case, so-called technological surprise (Handel, 1987).

Given the Swedish Armed Forces' transformation of S&T and capability development processes as outlined above, and the review of the technical forecast specifically, this study therefore asks the question: *How should forecasts concerning the military utility of technologies be formulated to be beneficial?*

This is an initial report from the study presenting a proposed framework to be used in evaluating the communication of technical forecasts to capability development activities. In the continuation of the study, the framework developed from the Swedish case will be used to identify experiences from similar communications in other contexts.

First, we describe our methodology; then, we present the Swedish Armed Forces' theoretical and conceptual foundations identified for capability development; then, we present related foundations from having a socio-technical systems-perspective; Last, the results are discussed, and a proposed framework is presented.

Methodology

First, we identify and formulate theoretical and conceptual principals - *foundations* - assumed to be of central significance for successful communication of technical forecasts, both from the perspective of how the Swedish Armed Forces view capability development and from a socio-technical systems view of military technology development. To identify the primary foundations for capability development of the Swedish Armed Forces, we review established guiding documents for knowledge development.

With effective communication in mind we successively analyse these foundations using a simple sender/receiver model as a lens to identify the interests of the producer of new knowledge and the consumer, respectively. The former is typically a researcher commissioned by the Swedish Armed Forces and the latter is typically an officer or analyst in the Swedish Armed Forces developing a new capability concept. In forming a framework, these interests are formulated at the end of each sub-section as questions denoted with “P#” for the producer and “C#” for the consumer.

The Swedish Armed Forces' Theoretical and Conceptual Foundations for Capability Development

In this section, the intention is to identify the theoretical and conceptual foundations that the Swedish Armed Forces use for their capability development, which we assume are significant

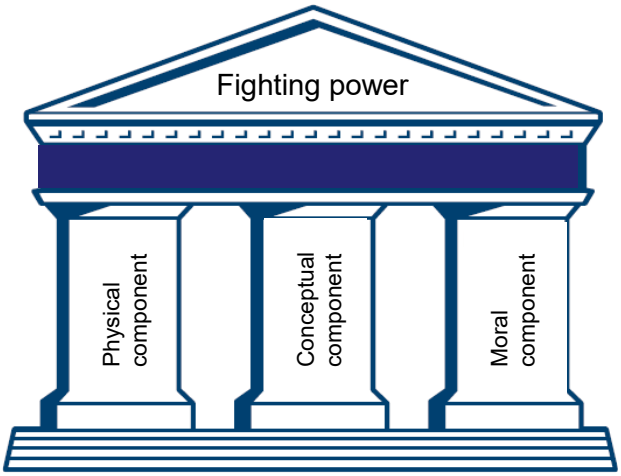
for how a forecast about future technological development is received. Each presentation concludes with a brief discussion from the study's socio-technical defence systems perspective and derived conclusions regarding the producer's (P) and consumer's (C) interests in the dialogue about the technical forecast.

Capabilities are viewed as Systems Dependent on Their Environment

Capability is central to V defence force's assessments and decision-making. There is a multitude of different definitions (Yue & Henshaw, 2009; Lindbom et al., 2015; Andersson, 2020), but the lexical definitions are usually formulated as the ability to do something or having the prerequisites to solve a task (Merriam-Webster, 2020; the Oxford Learners Dictionary, 2020.

The Swedish Armed Forces have long used the concept of *Krigföringsförmåga ("war-fighting capability")* in doctrines, where the Anglo-Saxon counterpart is *Fighting Power* (e.g., DCDC, 2014). The concept has in Sweden become well established, to the extent that to many in the armed forces it has become synonymous with the general concept of capability. Definitions have shifted somewhat over time, but the concept is typically illustrated as a temple supported by pillars representing three interrelated factors: physical, conceptual, and moral factors (Figure 1).

Figure 6.1: *illustrates the concept of Fighting power, or in Swedish, Krigföringsförmåga*



Source: (Swedish Armed Forces, 2016, p. 15)

The version adhered to in this study is taken from the strategic directive, FMSI 2021 (Swedish Armed Forces, 2021a), and it reads (translated):

> "Military fighting power is the sum of conceptual, physical, and moral factors – the combined capability to conduct warfare. The balance, as well as coordination and coherence, between the factors is crucial:

- Conceptual factors reflect the human side in ways of thinking, prescribing action – doctrine and legislation, ways of creating order and structure.
- Physical factors reflect the physical assets of the combat forces in the form of personnel, materiel, and infrastructure.
- Moral factors reflect the human side in will, courage, resilience, cohesion, learning, training, exercises, and leadership." (Swedish Armed Forces, 2021a)

Fighting power has thus, since its conception, been described as an effect of a whole consisting of interacting elements, in other words, as a system. The concept has the advantage of being used to reason about capability contributions from values difficult to measure, such as courage and determination. The authors have not been able to trace the theoretical origin, but it stems undoubtedly from early military theorists' observations on the importance of commander and morale for the outcome in battle, like Sun Tzu (1994) and Carl von Clausewitz (2006). In later editions of Swedish military strategic doctrine, the systems perspective has developed further. Fighting power is now described in accordance with the study's defence systems perspective as an open system, where it always must be assessed in relation to the external environment, especially in interaction with an adversary (Swedish Armed Forces, 2016, p. 16).

For the technical forecast, a view on capability based on the concept of fighting power means that a future technology must be assessed as a component in a military capability system, which in turn depends on the operational context or future operational scenario. However, the disadvantage of the intangible components in the concept of fighting power becomes apparent in production management contexts. The established interpretation of the concept of fighting power above is difficult to reconcile with the need to direct and monitor capability development. The next two subsections show how the concept has evolved to address these management issues.

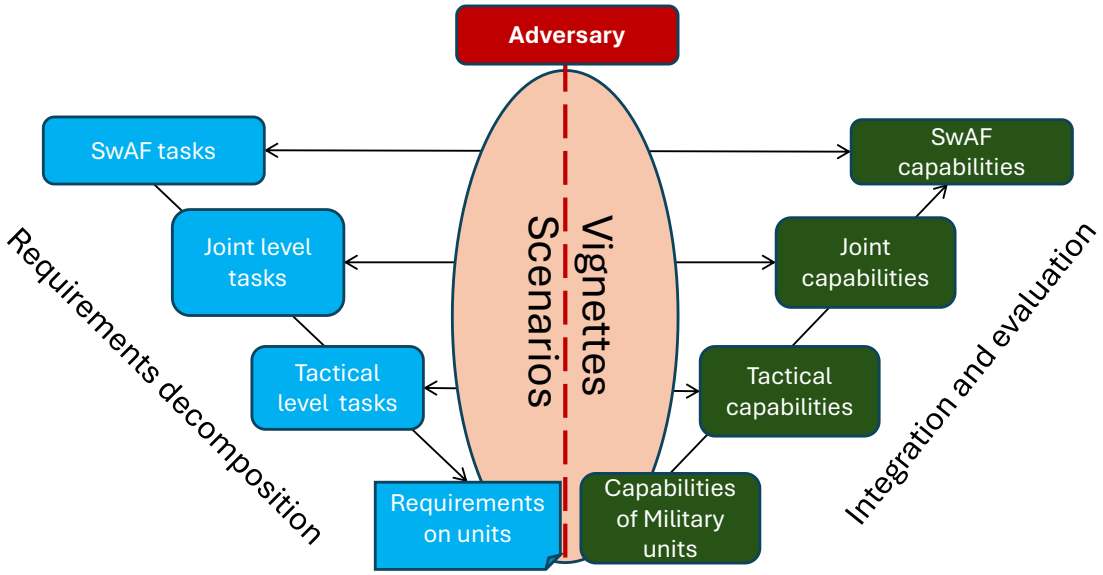
Derived interests in the dialogue:
P1: *What capability is relevant to consider in the assessment of the future technology in focus, and in what operational context should it be evaluated?*
C1: *Which capability development activities are affected by the forecast?*

In a management perspective, capabilities are hierarchically structured relative to tasks at different command levels

In the aftermath of the end of the Cold War the perspective on capability has evolved from a management standpoint. In the absence of a clear threat and a defined adversary, the western world developed a concept called [CBP], Capability Based Planning (Department of Defence,

2008). Instead of assessing capability against a well-known adversary, actors plan against a balanced portfolio of different capabilities. An advantage often highlighted is that with CBP capabilities can be described independently of their technical solutions and instead focus on solving the various tasks of the military actor (Fitzsimmons, 2007). Countries and defence alliances break down their capabilities into different abstract system components. The British classify eight Defence Lines of Development: "Training, Equipment, Personnel, Infrastructure, Concepts & Doctrine, Organization, Information, and Logistics" (Yue & Henshaw, 2009). The US have "Doctrine, Organization, Training, Materiel, Leadership and education, Personnel, and Facilities" (DoD, 2020), while NATO adds Interoperability (NATO, 2018). This concept for capability is used under the acronym DOTMLPFI. Regardless of the division into component categories, it becomes even clearer that no single component alone solves military tasks. Technical equipment must be operated by well-trained personnel organized to support appropriate doctrine for the desired effect to be achieved.

Figure 6.2: *illustrates the Swedish Armed Forces' Traceability Model*



Source: adapted from the Swedish Armed Forces (2021c).

The Swedish Armed Forces' production management has adopted this management perspective on capability. This is described in parts, for example, in the handbook for the Swedish Armed Forces' goal-setting process (Swedish Armed Forces, 2011) and the handbook for technical systems development (Swedish Armed Forces, 2013), as well as in the Traceability Model (Swedish Armed Forces, 2021d). Figure 2 illustrates how this perspective creates traceability between the Swedish Armed Forces' tasks and capabilities. The well-known (in management science) V-model (Forsberg & Mooz, 1998) is used to show how the military-strategic tasks are

gradually broken down into requirements for solving tasks at the operational level, which in turn are broken down into requirements for solving tasks at the tactical management level, etc. At the lowest level, the solution of these tasks can be specified in a goal-setting document for a typical unit. At the bottom of the V, the development of the military unit that will solve the corresponding tasks then occurs. On the right side, it illustrates how military units are integrated to solve increasingly complex tasks progressively. At each management level, the inherent capability of the increasingly complex units to solve tasks at the same level is evaluated. We also see that the evaluation depends on and occurs against a specified adversary in a specified context described by scenarios and vignettes. In the SwAF S&T directive (IFoU 22-25), this is summarized as "The Swedish Armed Forces are a system of systems where the capability of the constituent system components is recursively interdependent." (Swedish Armed Forces, 2021c, p. 6)

We can observe that the military theoretical perspective on capability, as described in the Swedish Armed Forces' military strategic doctrine, and the management science perspective on capability, as described in the Swedish Armed Forces' production-oriented documents, complement each other and share much in common. Both express a need to describe capability as the systemic effect that arises from the interaction between components divided in various ways, including technology, and that it must be evaluated in its current environment. However, the DOTMLPFI concept has advantages over the concept of warfighting capability in that the traceability between tasks and capabilities is clearer, and the constituent capability components are more tangible. Overall, the DOTMLPFI concept supports planning and monitoring of capabilities' successive development. With this perspective on capability, it follows that certain technical systems, or constituent technologies, support a specific level of command and environment more than others. Technologies for increased combat effectiveness, for example, typically have their primary impact at the tactical command level, while technologies for information gathering and dissipation often have their primary impact at higher command levels.

Derived interests in the dialogue:

P2: *Which level of capabilities is the focus, and what limitations or impacts from levels above or below should the assessment consider?*

C2: *Is our capability in focus (our study) influenced by the assessed technology, directly or indirectly?*

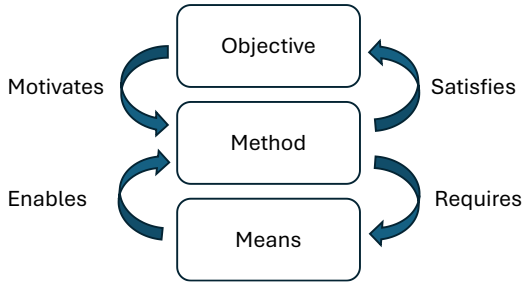
Development reveals a dynamic relationship between capability components

However, in the Swedish Armed Forces' strategic directive, FMSI (2021a), the military theoretical concept of warfighting capability has been chosen as the framework for capability development. In underlying production management documents, there is therefore a need to transfer the concept into a management perspective. Given the purpose of this study, to develop knowledge support for the Swedish Armed Forces' capability development, we choose to identify the recipient's understanding of capability in accordance with what is stated in the Swedish Armed Forces' directive for S&T (IFoU 22-25). There, capability components are defined to include:

- "Physical factors (what) reflect the material side of combat forces in terms of numbers, equipment availability, and technological level. Physical factors establish the conditions for what is possible to achieve, determining the means available. Physical factors are the easiest to discern, measure, and compare.
- Contextual factors (how) reflect the human side in terms of thinking, prescribing action— doctrine and regulations—and ways to create order. Conceptual factors guide education, exercises, and training, shape behaviours and methods, selection and application of means, and thus also shape what will practically be achieved.
- Moral factors (why) reflect the human side in terms of will, courage, leadership, resilience, ethics, and similar aspects. Moral factors motivate objectives and conceptual positions." (Swedish Armed Forces, 2021b)

We see that the principles behind the DOTMLPFI concept have been incorporated into the contextual factors, and that the moral factors have been made tangible by transferring them to objectives. Furthermore, IFoU (Swedish Armed Forces, 2021c) emphasizes that the continuous and mutual dependence between capability components means that all parts need to be considered simultaneously. These dependencies could thus form a figure that looks like the number eight, suggesting that change is continuously ongoing. The capability model in the Swedish Armed Forces' knowledge development that supports capability development is therefore described using the relational diagram in Figure 3. We see that “Means” in a bottom-up perspective enable “methods” to achieve “objectives”, while in a top-down perspective, objectives motivate the selection of methods. These, in turn, require access to means. Capability development occurs through decisions to change any of the three parts, resulting in impacts on dependencies and a new situation arising. In this representation, we henceforth refer to the model as *the Development-eight*.

Figure 6.3: *illustrates the dynamics between capability components. The relational diagram, referred to here as the Development-eight*



Source: adopted from the Swedish Armed Forces' S&T directive (Swedish Armed Forces, 2021c).

The dynamics illustrated by the Swedish Armed Forces with the Development-eight can be likened to how capability development is influenced by an effect often referred to in innovation research as technology push and demand pull (Di Stefano et al., 2012). The implication for this study is that capability development requires continuous collaboration and information exchange among all development activities sharing the same decision horizon, regardless of whether they focus on a technology or a method concept. Another aspect of this dynamic is, of course, the impact that the introduction of the new capability concept can have on an adversary. This phenomenon has long been recognized as a result of the dynamic interaction between military actors (van Creveld, 1991; Clausewitz, 2006). However, decision-making regarding this latter aspect is considered beyond the scope of the technical forecast.

Derived interests in the dialogue:

P3: *What requirements does the assessed capability concept impose on the technology in focus, and what possibilities for new or changed capability concepts does the technology enable in the opposite direction?*

C3: *How would our capability concept (our study) be affected by the new technology, or might the application of the new technology even enable a new capability of interest to our development activities?*

Capability development occurs across multiple decision horizons simultaneously - but is always implemented here and now.

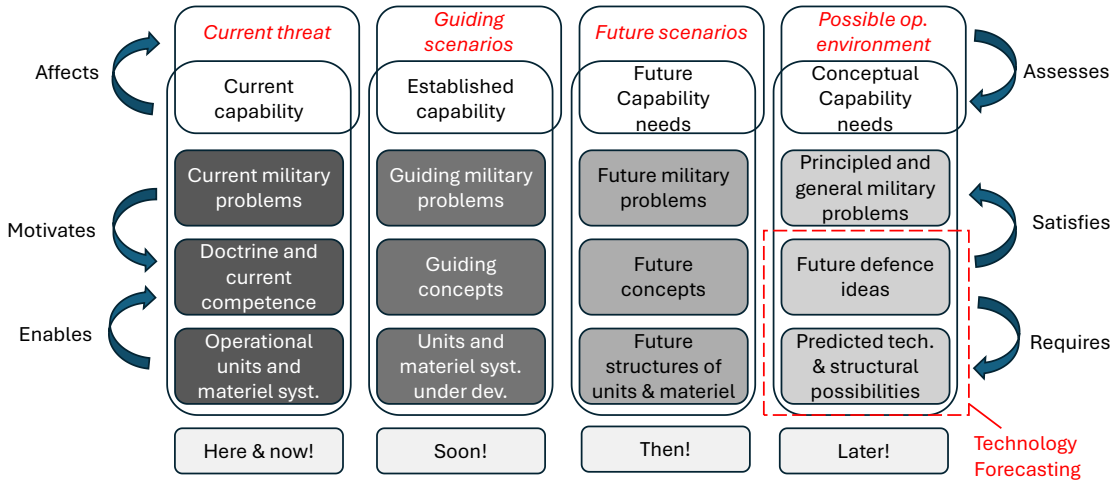
The current military capability of, for example, the Swedish Armed Forces can at any given moment be seen as the result of the Armed Forces' cumulative activities up to that point. However, the Armed Forces also engage in activities aimed at shaping tomorrow's available capability. In this study, we refer to the latter activities summarily as capability development. Given the DOTMLPFI perspective on capability, we can view it as the result of, among other things, materiel development, unit development, unit production (training, exercises), and organizational

development. If we view development as a conscious and active change of one or more aspects, aimed at making something better, we can understand capability development through the Development-eight as the conscious and active changes of means, methods, and objectives that a military actor undertakes to more successfully accomplish their tasks.

Furthermore, inherent to capabilities is their perishability. Without system (materiel) development, physical assets become obsolete over time, partly because adversaries' materiel advancements render their systems superior. Without unit development, the ability to effectively use available assets diminishes in the operational environment relevant at the time the capability is to be used. Without unit production, including training and exercises, units lose competence, for instance due to retirements leading to loss of acquired skills. And without organizational development, units and capabilities become irrelevant over time as the operational environment changes.

Considering the operations involved, we realize that capability development necessarily occurs across multiple decision horizons simultaneously. It is against this backdrop that we should understand the Swedish Armed Forces' categorization of capability development into four decision horizons according to the model in Figure 4 (Swedish Armed Forces, 2021a, 2021c).

Figure 6.4: *illustrates a model of capability development where the development-eight is placed in a context represented by scenarios and described across four decision horizons: here and now, soon, then, and later. In a Swedish context, typically five years are added for progressively longer decision horizons, corresponding to the political strategic defence review period.*



Source: The image is an evolution of "planning horizons" in the SwAF strategic directive (Swedish Armed Forces, 2020: p. 26) and is derived from the SwAF S&T directive (Swedish Armed Forces, 2021c).

The decision horizon "Here and now" in the figure covers the development activities that have been decided upon and thus represents the aggregated capability currently available, i.e., existing capability. Future capability concepts serving as a basis for decisions are represented in

the model by the Development-eight instantiated with the objectives, methods, and means corresponding to each decision horizon. The "Soon" decision horizon describes the capability concepts representing the decided capability following upcoming defence decisions. The "Then" decision horizon develops capability concepts to be used for planning after the next decision. These represent the so-called future capability needs. The capability concepts furthest to the right in Figure 4 constitute the result of activities aimed at providing knowledge to the planning activities. They represent conceptual capability in a future plausible environment. In a Swedish context, with defence decisions every five years, the activities furthest to the right occur within a decision horizon of up to 20 years at most. Technical forecasting is a part of this. An important point is that regardless of the decision horizon, *all activities take place here and now* - and they require tailored knowledge support (Swedish Armed Forces, 2021c, p. 5,6).

Studying Figure 4 based on forecasted technical and structural possibilities (the result of technical forecasting) clarifies important relationships affecting the dialogue surrounding technical forecasts. The previously identified dynamics between capability components are highlighted for each decision horizon. We understand that the results of technical forecasts can lead to new future defence ideas for method concepts, facilitated by future technology, or requirements from future ideas for method concepts developed by other activities. Above all, it is recognized that the primary recipients of this information are found among all the activities studying the near-term future capability needs. It thus becomes clear that forecasts and evaluations of technologies are conducted in a different context than where the recipients normally work. Mixing decision horizons, and thus abstraction levels in descriptions of the components in the evaluated capability concepts, is therefore likely to lead to misleading results. A longer-term forecast is necessarily more abstract than a forecast with a shorter time horizon.

A limitation of the model in Figure 4 is that it does not specify the level of command at which development activities are conducted. As previously noted, future technology under scrutiny may simultaneously influence or be influenced by capability concepts at development activities at the levels of combat, tactical, operational, and strategic command. However, this relationship is described in greater detail in IFoU 23 (Swedish Armed Forces, 2021c, p. 7).

Derived interests in the dialogue:

P4: *Towards which decision horizon should the assessment be directed, and what level of abstraction is most appropriate?*

K4: *What level of maturity is predicted for the technology at our decision horizon, and are the assumptions regarding the potential future environment comparable to our future scenarios?*

A socio-technical defence system perspective on forecasts of future technological development

In this section, the intention is to present the theoretical and conceptual foundations we have assumed are relevant for successful communication of technical forecasts given our socio-technical systems perspective on military technological development. Conclusions regarding interests in the dialogue surrounding technical forecasts are reported in the same manner as before.

The military utility of technology is assessed with the technology applied as part of a capability within a context

A socio-technical systems perspective on capability means that a technical system can only be evaluated within the context of capability. This is crucial for how and in what operational environment an actor intends to use the technical system. Therefore, we must determine from whose perspective the evaluation is made and at what level of command. For example, a splinter protected patrol vehicle has some value for the tactical commander with tactical tasks, while it may have a different value for the operational commander responsible for operational mobility. When we then assess the technical system, it is done in three dimensions. Firstly, regarding how effective the technical system is within its capability context, secondly, how well it integrates with other capability components in, for example, the DOTMLPFI concept, and thirdly, to what extent we can afford to procure and operate the system. We then say that we assess the military utility of the technical system (Andersson et al., 2014). Previously, it has been more common to settle for an assessment of the cost-effectiveness of the technical system, for example, through a system analysis (Roxström & Steen, 2020). The advantage of instead evaluating the so-called military utility is that it inherently considers legacy and the need for adaptations to tactics and training. The concept of military utility fits well with the Armed Forces' management perspective on capability. An assessment provides a basis for decisions regarding which technology should be considered in a development activity.

Regarding the dynamics highlighted by the Armed Forces in development, support from the concept is not as convincing. An objective-driven assessment of the military utility of a technical system (a means) top-down in Figure 3 implies that we first define a scenario and describe how the task is solved and then evaluate how well the technical system in focus meets the requirements. Critics argue, among other things, that such an assessment does not indicate the usability of the technical system in an emerging, previously unknown situation here and now

(Stensson, 2014). A means-driven assessment, bottom-up in Figure 3, instead starts from the available technical system to find the most suitable way to solve a task. The concept of military utility (Andersson et al., 2015) imposes no limitation (Silfverskiöld et al., 2021), but in designing an evaluation method, consideration must be given to the identified dynamic aspects. A possible solution is to let an evaluation be guided by the objectives the technology should contribute to solving, or to base the evaluation on the defined technical idea-system, whereby the utility is maximized through adaptations of method concepts and objectives. However, in the dialogue surrounding the technical forecast, a recipient should be aware of how these dynamic aspects have been considered in the evaluation of military utility.

Derived interests in the dialogue:
P5: *From whose perspective, at what command level, and in what operational context should the military utility of the technology in focus be assessed, and what dynamics can be expected?*
C5: *How high a priority should we assign to the forecasted technology in our study now, and when should we possibly revisit to follow up on its development?*

Projected technologies correspond to different degrees of integration

Next, it matters where on the scale between basic research and technical system our technology in focus is located when assessing its military utility. A technical concept or idea-system—such as cognitive radar—can often be readily integrated into a military capability and evaluated within that context (Swedish Defence University, 2019). However, in the field of technical forecasting, it is rare to assess fully developed systems with clearly defined functions. More commonly, the focus is on technologies that may be combined with others to form complete technical systems. Cognitive radar, for example, can be described as a combination of artificial intelligence and multifunctional radar technology (Karsten, 2018). To assess the military utility of artificial intelligence, one must first create at least one idea-system based on artificial intelligence and then assess that idea-system's military utility. Thus, the uncertainty in the assessment increases the further down the scale the technology in focus falls, because the assessment is based on an assumption about the practical possibilities of combining the different technologies. On the other hand, the value of the assessment also decreases because the technology in focus can likely be used in other idea-systems as well. This becomes even clearer if we decide to assess the military utility of technologies that support artificial intelligence, such as semiconductor technology. We do not believe any of the readers would object if we argued that semiconductor technology has significant military utility - but what value does such an assessment have?

Derived interests in the dialogue:

P6: *What possible combinations of technology or types of technical systems are of particular interest in assessing the military utility of the technology in focus?*

C6: *What other technical developments should we also pay attention to?*

The value of forecasts is affected by their uncertainties

The ability to make accurate forecasts of technological development and to assess the military utility of the projected technology are central parts of Technology Forecasting. Figure 4 gives us an idea of where it fits within capability development activities. The accuracy of technical forecasts is debated, but recent studies show that when done correctly, they can provide valuable decision support (Kott & Perconti, 2018; Silfverskiöld et al., 2021). Other researchers argue that defence forces should increasingly accept that they will be surprised on the battlefield and should therefore invest more resources in developing adaptability (Finkel, 2011). Our starting point is that we should do both. Given the purpose of this study, we therefore assume that the technical forecasts are well executed and instead ask how they should be formulated to maximize their utility in capability development.

To create an understanding of the nature of the uncertainties of these forecasts, we use an intelligence analytic framework for predicting developments in technology and defence (Clark, 1996). Here, a prediction of technological development is seen as the result of influence from a set of different influencing forces. By analyzing and taking these into account, it is often possible to make forecasts of technology and capability development with a good understanding of their uncertainties. The influencing forces are categorized as: organization, program, technology, capital, market, and regulations. An organizational analysis includes considerations of the actor's intentions, power distribution, efficiency, personnel supply, and decision-making processes; a program analysis involves predictions based on the actor's development processes; a technical analysis (if other than technology is forecasted) encompasses predictions of future performance of the technology in question, including supporting technologies, predictions of potential use and dissemination, and predictions of possible breakthroughs or innovations; a capital analysis addresses how innovations are put into production; a market analysis focuses on the strength and nature of market forces; and an analysis of possible regulations focuses on the influence of societal norms, laws, and other regulations.

Given a forecast of technological development, an assessment of its potential military utility is also required as a basis for the decision to introduce the technology into broader capability

development. With the perspective on military utility that we have chosen to use here, we recognize that the uncertainties in such an assessment stem from the combined uncertainties in the assessments of:

1) the future operational environment,
2) the effectiveness of the future capability in a given operational environment, with the focused technology as a component,
3) the opportunities to develop other components of that capability, and
4) the economic affordability of the technology.

Technologies with significant military utility for those who exploit them are sometimes referred to as disruptive, meaning they contribute to entirely new capabilities or make some previous capability obsolete (Bower & Christensen, 1995). Even if for some reason the Swedish Armed Forces choose not to exploit such technology, the assessment should be introduced to develop countermeasures and avoid technical surprises (Handel, 1987). Already when we outlined the concept of military utility above, we noted that the uncertainty in the assessment also depends on where on the scale between basic research and technical system our focused technology is located. Here, we want to highlight another aspect of this relationship. It is often combinations of different technologies that prove disruptive (Hundley, 1999). If we accept the description of increasingly rapid and extensive technological development, it is therefore reasonable to assume that innovations will emerge with greater frequency and shorter notice.

A forecast of technological development and the assessment of its military utility should therefore be accompanied by some estimation of the size and nature of the uncertainties. This reasonably affects the recipient's decision on whether to consider the forecasted technology in focus.

Derived interests in the dialogue:

P7: *What influencing factors and what societal or threat developments have a significant impact on the forecast and its uncertainties?*

C7: *Are the uncertainties in the assessment of the technology in focus acceptable, or what influencing factors and what societal or threat developments should we pay deeper attention to in our study?*

Conclusions

An assumption about seven central theoretical and conceptual starting points for dialogue around technical forecasts to support the Swedish Armed Forces' capability development has been

presented. From these, several interests have been derived. They have been formulated in the form of questions that either the producer of the technical forecast or the consumer can be assumed to have in the joint dialogue. By compiling these questions, a preliminary framework for effective communication around technical forecasts has been obtained in Table 1. In compiling the framework, some partially overlapping questions have been merged into a common one, which has been clarified with subsequent references where applicable. Generally, the word “capability” has been replaced by “capability concepts” with the intention of emphasizing ideas about future capability. The framework is expected to be further developed based on lessons learned in an upcoming study, where the intention is to apply it to empirical data.

Table 6.1: *Presents a preliminary proposal for a framework for analysing communication around technical forecasts within the context of capability development.*

Perspective	Interests	Ref.
Producer of technical forecast	Which management level and capability concepts are relevant to base the assessment of the future technology in focus on?	P1, P2, P5
	Given the relevant capability concepts, what limitations or impacts from levels above or below should the assessment take into account?	P2
	On what decision horizon, what level of abstraction, and in which scenarios from a possible environment should the future technology in focus be evaluated?	P1, P4, P5
	What requirements do potentially other components in relevant capability concepts place on the technology in focus, and what dynamics can be anticipated, i.e., what opportunities for new or changed capability concepts are expected to arise?	P3, P5
	Which potential combinations of technologies or types of technical systems are of particular interest in assessing the military utility of the technology in focus?	P6
	What influencing factors and societal or threat developments have a significant impact on the forecast and its uncertainties?	P7
The Consumer of the Technical Forecast (Studies and Concept Development)	Which study and concept development activities are directly or indirectly affected by the technical forecast?	C1, C2
	How would our capability concept in focus be affected by the new technology or could it enable a new one?	C1, C3

Perspective	Interests	Ref.
	What significance for the relevance of our study lies in the difference between the technical forecast's assumptions about the possible future environment and our future scenarios?	C4
	How high priority should we give the forecasted technology in our study now, and when should we potentially revisit its development?	C4, C5
	What other technological developments should we also pay attention to?	C6
	Are the uncertainties in the assessment of the technology in focus acceptable, or which influencing factors and societal or threat developments should we give deeper attention to in our study?	C7

Acknowledgements

This research was commissioned by the Swedish Armed Forces and the paper is developed from a report in Swedish. We used ChatGPT to improve our translation into English.

References

Andersson, K. *et al.* (2014) *Military Utility, a proposed concept to support decision-making*.

Andersson, K. *et al.* (2015) 'Military utility: A proposed concept to support decision-making', *Technology in Society*, 43. doi: 10.1016/j.techsoc.2015.07.001.

Andersson, K. (2020) 'Notes on military capability concepts and their relevance for analysis of system characteristics', 1(12), p. 12. Available at: http://fhs.diva-portal.org/smash/get/diva2:1473159/FULLTEXT01.pdf%0Ahttp://urn.kb.se/resolve?urn=urn:nbn:se:fhs:diva-9463.

Andersson, K., Lundmark, M. and Silfverskiöld, S. (2019) *The Military Utility Assessment Method for Future Technologies*. Stockholm. Available at: http://urn.kb.se/resolve?urn=urn:nbn:se:fhs:diva-8660.

Bower, B. J. L. and Christensen, C. M. (1995) 'Disruptive technologies: catching the wave', *Long Range Planning*, 28(2), p. 155. doi: 10.1016/0024-6301(95)91075-1.

Clark, R. M. (1996) *Intelligence Analysis: Estimation and Prediction*. Baltimore, Maryland: American Library Press, Inc.

Clausewitz, C. von (2006) *On War*. EBook edit. The Project Gutenberg. Available at: https://www.gutenberg.org/files/1946/1946-h/1946-h.htm#chap09.

van Creveld, M. (1991) *Technology and war*. New York, Toronto, Oxford, Singapore, Sydney: The Free Press.

DCDC (2014) *UK Defence Doctrine, Joint Doctrine Publication 0-01*. Shrivenham: UK Development, Concepts and Doctrine Centre.

Department of Defense (DoD) (2020) 'DOD Dictionary of Military and Associated Terms', *Joint Education and Doctrine Division, J-7*, (January), p. 382. Available at: http://www.jcs.mil/Doctrine/DOD-Terminology/%0Ahttps://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf.

DoD (2008) Directive 7045.20 Capability Portfolio Management.

Finkel, M. (2011) On Flexibility - Recovery from Technological and Doctrinal Surprise on the Battlefield. Stanford University, Stanford, California, USA.
Fitzsimmons, M. (2007) 'Whither Capabilities-based Planning?', *JFQ*, (44), pp. 101–105.
Försvarshögskolan/Swedish Defence University (2019) Technology Forecast 2019 : The Military Utility of Future Technologies.
Försvarsmakten/Swedish Armed Forces (2011) 'Handbok för Försvarsmaktens målsättnignsarbete, H MÅL Förb 2011', p. 56.
Försvarsmakten/Swedish Armed Forces (2013) *H FM Tek Syst Tekniska system - Definitioner och kostnadsberäkningar*. Stockholm: Försvarsmakten.
Försvarsmakten/Swedish Armed Forces (2016) *Militärstrategisk doktrin – MSD 16 2016*. Available at: https://www.forsvarsmakten.se/siteassets/4-om-myndigheten/dokumentfiler/doktriner/militarstrategisk-doktrin-2016-ny.pdf (utskriftsdatum 2018-10-24).
Försvarsmakten/Swedish Armed Forces (2021a) 'Försvarsmaktens Strategiska Inriktning 2021-2030'. Available at: https://www.forsvarsmakten.se/sv/om-forsvarsmakten/darfor-finns-forsvarsmakten/strategisk-inriktning/.
Försvarsmakten/Swedish Armed Forces (2021b) 'Inriktning av Försvarsmaktens forskning och utveckling 2022-2025 (IFoU 22)', p. 47.
Försvarsmakten/Swedish Armed Forces (2021c) 'Inriktning av Försvarsmaktens forskning och utveckling 2023-2025 (IFoU23) - bilaga 1', p. 56.
Försvarsmakten/Swedish Armed Forces (2021d) 'Missiv Beslut om U RVT, FM2021-17939-1'. Försvarsmakten.
Government offices of Sweden. (n.d.). Defence innovation. https://www.government.se/government-policy/defence-innovation/
Handel, M. I. (1987) 'Technological surprise in war', *Intelligence and National Security*, 2(2), p. 53. doi: 10.1080/02684528708431875.
Hundley, R. O. (1999) Past revolutions, future transformations: what can the history of revolutions in military affairs tell us about transforming the U.S. military? Washington D.C.: RAND. Available at: http://www.rand.org/.
Karsten, M. (2018) 'Cognitive Radar : Artificial Intelligence in Radar Systems'. Fraunhofer Institute for Technological Trend Analysis INT.
Kott, A. and Perconti, P. (2018) 'Long-term forecasts of military technologies for a 20-30 year horizon: an empirical assessment of accuracy', *Technological Forecasting and Social Change*, 137, pp. 272–279.
Lindbom, H. *et al.* (2015) 'The capability concept - On how to define and describe capability in relation to risk, vulnerability and resilience', *Reliability Engineering and System Safety*. Elsevier, 135, pp. 45–54. doi: 10.1016/j.ress.2014.11.007.
Modig, O. and Andersson, K. (2021) 'Military innovation as the result of mental models of technology (in manuscript)', *Scandinavian Journal of Military Studies*.
NATO (2018) 'AAP-06 Edition 2018 NATO GLOSSARY OF TERMS AND CONDITIONS'. NATO.
Nätzker, W. and Huppertz, G. (2017) 'Hypersonic propulsion, October 2017'. Fraunhofer Institute for Technological Trend Analysis INT.
O´Hanlon, M. (2020) 'Forecasting change in military technology 2020-2040', *Foreign Policy at BROOKINGS*. doi: 10.1093/ia/iiaa075.
Roxström, G. I. T. and Steen, L. (2020) 'Underlag till Försvarsmaktens handbok i studiemetodik 2020'.
Silfverskiöld, S., Andersson, K. and Lundmark, M. (2021) 'Does the method for Military Utility Assessment of Future Technologies provide utility?', *Technology in Society*, 67(September). doi: 10.1016/j.techsoc.2021.101736.

Di Stefano, G., Gambardella, A. and Verona, G. (2012) 'Technology push and demand pull perspectives in innovation studies: Current findings and future research directions', *Research Policy*, 41(8), pp. 1283–1295. doi: 10.1016/j.respol.2012.03.021.

Stensson, P. (2014) *The Quest for Edge Awareness - Lessons not yet learned*, Avhandling, Uppsala universitet.

Tzu, S. (1994) *The Art of War*. Ebook edit. The Project Gutenberg.

US Department of Defense (2008) *Capability Portfolio Management, Directive 7045.20*. Washington D.C.: US Department of Defense.

Yue, Y. and Henshaw, M. (2009) 'An Holistic View of UK Military Capability Development⋆', *Defense & Security Analysis*, 25(1), pp. 53–67. doi: 10.1080/14751790902749900.

Chapter 7: The impact of hybrid threats on operations in modern warfare.

Col. Viktor **Savchenko**, ORCID: https://orcid.org/0009-0008-7492-7438

Abstract:
The relevance of this paper stems from the evolving nature of warfare, marked by changes in forms and methods. This study analyzes the hybrid war the Russian Federation instigated against Ukraine. Characterized by a combination of actions involving covert deployment of regular troops, illegal armed formations, terrorist organizations, propaganda, sabotage, and terrorist attacks, this hybrid warfare model is expected to shape future armed conflicts, significantly impacting military operations. Hybrid threats pose challenges in identification and tracking due to their cunning and implicit methods. Commanders on different levels actively seek ways to identify these threats and protect subordinate forces. Hybrid threats directly affect the operation during its preparation phase and throughout conducting in a defined operational area. These threats can be typically divided into four levels of influence: political, legal, informational, and physical or kinetic (*directly related to human material loss*). The Russian Federation has initiated actions at the diplomatic level in advance, affecting internal political processes in Ukraine. These measures included creating a belt of instability, influencing and applying double standards, portraying Ukraine as a "Security Threat," actively interfering in elections, infiltrating agents of Ukraine's government and security structures, and stimulating corruption. The armed forces of the Russian Federation, whenever possible, avoided direct military confrontations and widely employed asymmetric actions, illegal armed formations, terrorist organizations, and criminal elements. At the same time, the deployment of regular troops (*forces*) was conducted covertly. All these measures at the legal level curbed the full exploitation of the Armed Forces of Ukraine. Russian propaganda, an artificial parallel informational reality, along with elements of cyber warfare are significant factors in influencing the information space of the population of Ukraine, the population of the Russian Federation, and the global community. Simultaneously, the Russian Federation employed sabotage, tactics of terror, sabotage, and the involvement of proxy forces to destabilize the situation and increase pressure on the military-political leadership of Ukraine. The paper aims to identify factors impacting armed forces' effectiveness under hybrid threat influence and the broader context of modern military conflicts. The study outlines key areas for commanders to address when countering hybrid threats during preparation and execution of operations.

Keywords: Hybrid Warfare, Ukraine, Information Warfare, Unrestricted Warfare

Introduction

Before 2022, political and economic globalization made large-scale warfare unlikely possible. However, some countries seek to revise the power distribution in the current competitive environment. They are looking into how to increase the influence on countries outside the conventional use of force. They are trying to avoid the modern configuration of the security environment. The most known example of this is the Russian Federation. Moscow successfully used tactics and techniques of irregular warfare and implemented "grey zone" activities in adjacent countries, including Lithuania, Moldova, Georgia, Ukraine, and Kazakhstan. Due to the lack of Russia's economic influence on the international stage, Russia has used hybrid and military means to strengthen President Putin's diplomatic voice. Russia has also forced an enduring competitive operational environment between countries' legal governments and non-state actors. Even without the conventional use of troops, Russia has cultivated grey zone activities in Ukraine in order to pursue Russian national interests. In this condition, stakeholders cannot neglect the fact that the use of hybrid threats – in addition to nuclear and conventional deterrence – can proactively shape conditions to achieve benefits in great power competition. The current environment of hybrid warfare makes existing doctrines and approaches to unconventional war less relevant and need adjustment. Moreover, international security organizations and alliances are not ready to curb hybrid threats because of comprehensive strains in the diplomatic, political, economic, informational, and social domains.

The so-called "Unrestricted Warfare" doctrine of China was described by Chinese military theorists Qiao Liang and Wang Xiangsui (Liang & Xiangsui, 1999). They highlighted modern approaches to waging war in the new geopolitical environment and emphasized that war is not limited to military actions - it covers a wider range of strategic, operational, and official and unofficial methods of influencing the enemy, such as economic pressure, information warfare, cyber-attacks, psychological operations, etc. The key idea of this doctrine is that in a modern armed conflict, combat clashes can take place in different theaters of operations at the same time, and it is necessary to use all opportunities to influence the enemy, not limited to conventional military actions. From the Russian perspective and according to the so-called "Gerasimov Doctrine," modern warfare combines military, technological, informational, diplomatic, economic, cultural, and other factors (Gerasimov, 2013). Gerasimov argues that to achieve a nation's strategic goals, it is practical to operate in all these domains, as contemporary conflicts include undeclared wars, a mix of military and non-military operations, and targeted operations by small forces (The United States Army Special Operations Command, 2015). Modern military experts view hybrid warfare as a combination of military, paramilitary, diplomatic, informational, economic, legal, and other means

to achieve strategic political objectives. The hybridization of actions involves using both military and non-military methods for military purposes and employing them as weapons (Koval, 2023).

This study employs a qualitative case study design, supported by elements of strategic analysis and thematic content analysis. The aim is to examine the impact of hybrid influence tools on the course of events in contemporary conflicts, using the Russia-Ukraine war as a paradigmatic example. Thematic content analysis was applied to identify recurring patterns and narratives concerning the use of diplomatic, legal, economic, informational, and kinetic tools in hybrid warfare. Strategic analysis was then used to interpret how these hybrid tools are integrated into modern operations against democratic states. Analytical frameworks from contemporary security studies were employed to assess the impact of hybrid measures on military potential, state resilience, and international relations.

Ukraine was selected as a critical case due to its impact on the European political landscape and the prolonged, multifaceted hybrid aggression from the Russian Federation. It represents a context in which economic, informational, military, and diplomatic tools are simultaneously employed to achieve strategic objectives. Focusing on Ukraine provides insight into the vulnerabilities and adaptive capabilities of democratic states under hybrid pressure. Data triangulation was used to enhance construct validity by cross-referencing official statements, statistical data, and third-party analyses.

Discussion

There is no universally accepted definition of the term “hybrid warfare.” One of the first scholars to conceptualize the notions of hybrid threats and hybrid war was Frank G. Hoffman (Hofman, 2007). According to Hoffman, hybrid threats represent a spectrum of different modes of warfare, including conventional military capabilities, irregular tactics and formations, terrorist acts (*including indiscriminate violence and coercion*), and criminal disruptions. He emphasizes that hybrid wars may be waged by both state and non-state actors.

In NATO analytical documents, hybrid warfare is defined as the combination of conventional, irregular, and cyber warfare, as well as the coordinated use of political, economic, informational, and diplomatic instruments (NATO, 2015). NATO experts highlight the integrated application of military and non-military means of influence, including cyber capabilities, information operations, and diplomatic tools.

Experts from the RAND Corporation, a prominent U.S.-based strategic think tank, view hybrid warfare as a convergence of diverse methods and instruments of warfare, employed in a complementary manner to achieve political objectives without formally declaring war (Chivvis,

2017). Chivvis particularly stresses the undeclared nature of hybrid war and its reliance on the combination of instruments aimed at influencing the target state without crossing traditional “red lines.”

The perspective of Ukrainian military professionals is presented in the monograph "Theoretical and Applied Aspects of the Russo-Ukrainian War: Hybrid Aggression and National Resilience" by Mykhailo Koval and colleagues. According to their definition, "Hybrid warfare is a combination of military, quasi-military, diplomatic, informational, economic, legal, and other instruments of influence used to achieve the political goals of an aggressor, often involving proxy forces and other indirect methods of coercion" (Koval et al., 2023).

Valery Gerasimov, Chief of the General Staff of the Armed Forces of the Russian Federation, introduced an informal definition. Gerasimov described hybrid warfare as the blurring of the lines between war and peace. He asserted that the "rules of war" have changed in contemporary conflicts, and non-military means have become central to achieving political and strategic objectives (Gerasimov, 2013).

Many experts believe that hybrid warfare combines traditional and unconventional tactics, combining the overt and covert use of a wide range of tools: military and civilian, conventional and unconventional, including information operations, diplomatic and economic pressure, and influence operations (Hofman, 2007; Heickerö, 2010; Wetoszka, 2016; Cullen, 2017; Theohary, 2018; Marsili, 2021).

Every state has defined legislation and military doctrine that outline how to respond to any hazards in peacetime and times of war. However, if we are talking about the Gray Zone, the space between peace and war, we can often see gaps in our military and political manuals. Sometimes, the victim state cannot realize the hostile activity at all. In some cases, victim states can detect these actions but cannot react to them because of the asymmetric nature of the means used or the absence of precise mechanisms on how to react. These imperfections create fertile soil for aggressors to use unconventional approaches against democratic states. For example, in the **diplomatic domain**, we can talk about some kind of delusion to keep a friendly relationship with the aggressor. At the same time, the foe uses the politics of non-provocation and non-escalation and prepares the ground for future war. In the **informational domain**, we can see how the aggressor creates a powerful information impact on the victim state, its own population, and the international society. However, just using propaganda is not a case to count as hostility. Some activities in **the economic domain** can significantly limit the possibilities of the victim state building a military-industrial complex and provide modernization of the armed forces.

The Russia-Ukraine war gave us a bright example of how to start a war without using governmental organization, and armed forces. Russian Federation actively denied using its own forces in Crimea in 2014 and late in Donbass up to 2022. Moscow used narratives and fairytales about local self-defense forces, patriotic organizations, and "*little green men*" to cover of use of special operational forces and the regular army. Aggressor-country often actively impose the status of conflict to take advantage. The common practice for aggressors is to cultivate local conflict or civil war inside the victim country. This conflict allows the aggressor to choose a legal place such as to be a supervisor or worried witness, not a participant. This situation prevents the International Society from applying international sanctions and condemnation.

Using unconventional methods and techniques of warfare helps the aggressor country. At the same time, the aggressor has an opportunity to support its politics, destroy infrastructure and governmental institutions inside the victim country terminate or disable armed forces, and prepare the population and international society for future intervention. The uncertainty of the situation provides the aggressor state with different ways for future action, such as carrying out military peacekeeping operations, providing local military action, allegedly to defend local minority populations that are being genocide by the government, or just having a long-term local conflict that can be used in the future to exhaust the victim country. To effectively assess the impact of hybrid threats on military operations, it is crucial to examine the key domains where these threats manifest: Political, Legal, Informational, Economical, and Kinetic. These domains and the methods used within them demonstrate how hybrid threats are complex and multifaceted, aiming to weaken the target national armed forces from multiple angles without relying solely on traditional military engagement. Let's look at these tools more thoroughly.

At the political level, an aggressor nation often seeks to advance its interests by establishing a **zone characterized by instability**, influence, and inconsistent standards around its borders. The aggressor may use internal diversity—whether based on religion, ethnicity, or politics—to raise social instability and advocate for its own interests. A common tactic is the deployment of peace and **anti-militarization rhetoric** ostensibly to ensure regional security and prevent a resurrection of Cold War-era and arms races. Such narratives are designed to lower the vigilance of neighboring countries, creating conditions where the aggressor portrays any defense improvements within the target nations as threats to regional peace and stability. Consequently, this strategy places the military-political leadership of the target nation in a risky position, potentially limiting military capabilities to build and prepare for future conflict. The aggressor may also exploit the pretense of protecting ethnically aligned civilian populations from nationalists and perceived injustices by local authorities. The aggressor may further implement a strategy of **non-**

provocation through continuous intimidation, threats of retaliatory actions, and nuclear blackmail. These measures can be a part of a hybrid influence campaign targeting both the population and military leadership of the victim country, as well as the global community. This strategy aims to deter support and weapon provision, coercing the military-political leadership into concessions. Democratic systems, characterized by open access to information, pluralism, and media freedom, are particularly vulnerable to hybrid warfare tactics. Information operations against opposing candidates, voter bribery, and cyber-attacks on electronic voting systems are frequently employed by the aggressor's special services to **manipulate electoral processes**.

Another aspect of hybrid warfare involves **infiltration into governmental** and power structures. Aggressor countries may provide direct support to specific political groups or actors within the target country, sometimes through official channels or international engagements. Covert or semi-official support for protest or separatist movements, including financial backing and information dissemination, helps create a destabilizing "fifth column" or network of influence, facilitating the aggressor's strategic objectives without using force (Chivvis, 2017). **Traditional espionage** remains a significant political-diplomatic tool in hybrid warfare. Under diplomatic cover, special services may engage in bribery, blackmail, and other coercive tactics against political figures. The impact of such influence can be profound and enduring, with long-term consequences for decision-making even after the identification and removal of compromised officials. **Corruption** represents a fundamental threat, undermining economic stability and increasing inequality, thereby diminishing public trust in national institutions, including the military. Corruption schemes and scandals, opposition to anti-corruption measures, and accusations against military leadership erode the integrity of the armed forces and the overall defense capability, ultimately affecting national security and Armed forces morale.

At the legal level, hybrid warfare tools are used to either prevent or restrict the use of force due to the lack of legal foundations. The aggressor may involve **avoiding direct confrontations** with the armed forces of the victim country by using asymmetric and non-linear actions. The activities of anonymous, well-organized, and trained special groups from locals and mercenaries can significantly influence the situation at the onset of a crisis. Some of these groups' actions may focus on distorting the image of the national Armed Forces, police, and national activist movements. These actions can be directed at both the population of the victim country and the international community. The **cover-up of the armed forces' involvement** as an official state institution provides the aggressor country with an advantage. First, it affects the victim country's society, which, in the absence of a proper assessment of the situation with relevant evidence of the aggression, will attempt to delay making decisive and unpopular measures to protect its

sovereignty. Second, the international community, under the influence of distorted propaganda and misinformation, will be unable to provide comprehensive support to the country -victim of hybrid aggression. To advance its geopolitical projects, the aggressor country may option **to use illegal armed groups, terrorist organizations, or private military companies** [PMCs]. Typically, PMCs serve as unofficial (*and in most cases illegal*) foreign policy instruments. Recent conflicts have shown that military activity in the victim country often **begins without a formal declaration of war**. There were no legal or diplomatic procedures under international law, that involved one state officially notifying another of the cessation of peace and transition to a state of war. This allows the aggressor country to avoid sanctions from the international community for as long as possible.

Another tool of hybrid warfare is **criminal activities.** In the war in Ukraine, **numerous criminal activities** such as intimidation, bribery, and murder have been documented. According to UN reports, these actions were mostly carried out by armed formations operating in occupied territories or supporting the conflict. These crimes, committed against both civilians and military personnel, aim to destabilize the situation both within the country as a whole and directly in the combat zone. Transnational organized crime can be involved in zones of conflict and increase the number of victims and exacerbates global challenges, from migration to cyberattacks. It undermines the security and stability of entire regions, erodes the rule of law, fosters corruption, and acts as an intermediary for hostile state activities (White House, 2022).

Another powerful tool of hybrid warfare is **narratives regarding the illegitimacy of the conflict**. Various combinations of historical distortion regarding the basis of state existence are repeatedly voiced by the aggressor country at all levels, from the president to hired bloggers. The charge of illegal seizure of power is emphasized in order to deprive the government of the victim country of its legal status. Claims of supposed self-determination by the population are also used to attempt to confer civil war status on the conflict and portray the national government and armed forces as criminals. These narratives affect politics and decision-making processes, the ability to govern the state, the morale of the military, obedience to orders, and support from local and international economies. The combination of psychological operations and political actions shapes the behavior of the target audience in the victim country to support the aggressor country's policy objectives and affects the command's intentions at strategic, operational, and tactical levels (Headquarters Department of the Army, 2003).

An important layer of hybrid warfare is the symbiotic connection between the hybrid aggressor and the modern information environment that includes all possible mass media and social networks. The ability to exert total online informational influence on society gives hybrid

warfare a different meaning. The informational space has transformed into a battleground, and information has become a weapon with a very real destructive effect, not destroying physical objects, but rather altering perceptions of reality (National Academy of the Security Service of Ukraine, 2021). For example, the Russian Federation has used propaganda to cause political instability and poison neighboring countries in order to regain regional dominance and counter the influence of the collective West (Marsili, 2021). This activity had started much earlier, before the invasion of Georgia in 2008 and the annexation of Crimea in 2014. Information warfare blurs the line between peace and war, and goes beyond traditional warfare to the intersection of information, physical, and cognitive-social spheres (Bishop, 2003). Thus, the boundaries between "traditional" and "unconventional" warfare are blurred, and even the line between the physical, kinetic, and virtual dimensions of conflict is blurred (Marsili, 2021).

The main directions of informational activities targeting Task Forces may include **propaganda** through mass media and various online resources, operations of deception and disinformation, agitation of military personnel through hidden local and professional foreign agents, and the creation of a Russian artificial parallel informational reality. These activities aim to shape the assessment of the situation and decision-making process at all levels of military leadership, as well as to exert continuous cyber influence on military personnel, command and control systems, and maintenance operations. According to the concept of total war, the military phase of aggression is always preceded by a long, latent period of informational aggression. Propaganda is a powerful tool used by an aggressor country. Propaganda targets military personnel, intelligence officers, journalists, diplomats, and politicians, drawing them into the informational war. For example, modern Russian propaganda aims to convince society that truth simply does not exist. The main task of propaganda is to keep the audience in a suspended state of half-truth. But if truth does not exist, then anything is possible (National Academy of the Security Service of Ukraine, 2021). Thus, the Russian interpretation of reality is often more focused on undermining narratives of democratic countries than on presenting a constructive Russian counter-narrative. An important tool of hybrid warfare in supporting targeted political or military actions is deception and disinformation operations. The aggressor country will constantly try to influence the informational space of both the victim countries and the international community. The general vectors of this influence may include concealing true intentions, covering up actions, hiding failures and miscalculations of military-political leadership, and creating informational chaos to obscure critical information (*such as various versions regarding the downing of Malaysian flight MH-17*) (Horbulin et al., 2009).

Factors such as inadequate moral values and freedom of the democratic media, internal corruption, and the oligarchic nature of the media system make the victim country vulnerable to hostile informational influence. This influence can be carried out through **agitation by hidden local and professional agents** and can be present in various spheres of public life, working through non-governmental organizations, pseudo-patriotic, and religious organizations. A priority informational goal for the aggressor country may be to create an **artificial parallel informational reality** where only narratives favorable to the aggressor prevail. The aggressor country should accompany its operations with highly effective tools of informational influence, such as television, radio, and social media with qualified personnel, including "activists" and so-called independent bloggers, and involving professional actors. Dominance in the informational space will help the aggressor distort the real situation in the victim country for both the international community and the internal audience (The United States Army Special Operations Command, 2015). Modern society and the critical infrastructure that supports it are becoming more digitalized and vulnerable to disruptions or informational influence through cyberattacks. Hackers will regularly attempt to disrupt the operation of governmental and military institutions in the victim country. The goals of the attacks may vary, such as financial gain: ransom for restoring systems or data theft for sale, informational dumps, disabling alert and control systems. From the experience of the war in Ukraine, often they are coordinated with military operations. Hybrid warfare's psychological component targets the adversary's decision-making processes, aiming to induce self-doubt and errors. Techniques include strategic misinformation, diplomatic pressure, false interpretations, and harassment, all designed to generate anti-war sentiment among the population, sway electoral outcomes, and undermine social resilience. Psychological operations are employed to erode society's will to fight and encourage self-criticism.

In the context of hybrid warfare, the economic dimension plays a critical role in shaping the strategic environment and influencing the resilience of the target state. The material component - including the availability of military equipment, defense investments, and the development of the military-industrial complex [MIC] - must be assessed in conjunction with national perceptions of strength and vulnerability, as well as the need to satisfy state-specific socio-economic demands. These factors are key to understanding the probability and trajectory of a potential conflict. Hybrid economic pressure employs various instruments such as economic sanctions, border closures, and the targeted disruption or degradation of MIC infrastructure. These measures aim to weaken a state's defense capabilities and contribute to broader destabilization efforts. Notably, Russian Foreign Minister Sergey Lavrov characterized the Western sanctions imposed following Russia's

invasion of Ukraine as a “real hybrid war” and a declaration of “total war,” (TASS, 2022) thus acknowledging the strategic role of economic tools in modern conflict.

The **blockade** of Ukrainian **borders**, coupled with export-import restrictions—including those related to the Black Sea Grain Initiative and the so-called "grain wars"—had a substantial impact on the dynamics of the war. These disruptions directly undermined Ukraine’s economic sustainability, military supply chains, and international backing. The agricultural sector, contributing approximately 20% to Ukraine’s GDP and up to 45% of its export volume, became a primary target of hybrid economic attacks. The loss of key southern agricultural territories and the subsequent 50% reduction in grain exports led to a sharp decline in foreign exchange revenues (Braun, 2025). This, in turn, limited Ukraine’s capacity to fund its armed forces, implement social welfare initiatives, and carry out critical infrastructure restoration. **Maritime blockades**, particularly of the Odesa port, rendered swift naval delivery of arms and humanitarian aid infeasible, complicating military logistics and increasing reliance on overland transport routes. However, these alternative routes—especially those crossing western borders—were often congested or obstructed by protests, as observed on the Polish Ukrainian frontier (INFORMS, 2025). Such logistical bottlenecks slowed the transfer of essential military hardware and supplies. **The economic blockade** also produced notable geopolitical repercussions. Russia's withdrawal from the Black Sea Grain Initiative in July 2023 precipitated a global food crisis, particularly in African and Middle Eastern nations. While this crisis mobilized diplomatic support for Ukraine, it also strained bilateral relations with neighboring countries (*e.g., Poland*) due to the EU’s support for Ukrainian food exports, which some local markets viewed as economically disruptive (Dodd, 2024). Russia’s manipulation of food security represents a calculated tactic within its hybrid warfare arsenal, designed not only to impair Ukraine financially but also to generate external pressure on Western allies by fostering instability in partner states (Scheuerman, 2023). In conclusion, border blockades and trade restrictions function as strategic instruments within the broader spectrum of hybrid warfare. Maintaining economic and logistical stability in the face of such challenges is vital for ensuring national defense readiness and sustaining international coalition support.

At the Kinetic level, we have a combination of tools of unconventional warfare and modern technology. The aggressor country may carry out **terrorist attacks** on critical infrastructure to intimidate the civilian population in the victim country long before the active phase begins. This terror is intended to create pressure on the government of the country from civilians, leading to capitulation or at least concessions to the aggressor. Terroristic attacks on infrastructure facilities, aimed at disrupting the normal functioning of services and systems at the initial stage, also have

a powerful effect. After the active phase begins and the national consciousness of the people grows and their vigilance increases, carrying out such sabotage becomes increasingly challenging.

Sabotage can be not only military action. Throughout 2023-24, a group of Polish farmers sabotaged the implementation of a bilateral agreement and demanded the cancellation of visa-free transportation between Ukraine and Poland (Zanuda, 2014). Officially, the Ukrainian government did not receive demands from either the Polish farmers or the Polish government. Overall, their demands largely fall outside the jurisdiction of the governments of Ukraine or Poland, and some of the demands are illegal. However, such acts on major supply routes for weapons from partner countries to Ukraine complicate military logistics and directly impact the conduct of military operations. In modern conditions, the use of armed forces is internally provocative for the state and may trigger international sanctions.

Hybrid tools allow the aggressor country to deny responsibility for any actions on the territory of the victim state. **Proxy forces** have the status of non-state actors. Private military companies [PMCs], non-governmental funds and support associations, and pseudo-patriotic organizations are widely used as hybrid tools in different military conflicts in Ukraine, the Middle East, and Africa (Russell, 2021). The most well-known of PMC is the Russian Wagner Group. It should be noted that the Wagner Group is a conglomerate of organizations, including media, military formations, and cyber-influence institutions (*bot farms*). The Wagner Group offered their customers a full range of "security service regime" services, including propaganda and information operations. Actually, in future warfare, PMC deployment can serve as an alternative to conventional armed forces in both official and undeclared conflicts. The Wagner Group has been linked to numerous human rights violations and war crimes in Ukraine and African countries (Congress Research Service, 2013). This PMC had a significant influence on domestic political processes in these countries. With full support from security structures and state backing, the use of PMCs enables intervention in the internal politics of other countries using criminal and terrorist methods without incurring international sanctions against the aggressor country.

The list of hybrid warfare tools is constantly expanding. The situation at the Belarus-Poland border in 2023 showed us that refugees and displaced persons can be used as weapons. Moreover, the use of migrants for political purposes is seen as a hybrid move that leads to diplomatic and economic sanctions, but not to a military response (Marsili, 2022). European Commission President Ursula von der Leyen held Belarusian authorities responsible for a “hybrid attack” during the border conflict between Poland and Belarus in November 2021. The UN Security Council has described the “orchestrated use of people for political purposes” as a “hybrid operational tactic” (Von der Leyen, 2021). In the context of total war, artificially directed refugee

flows in a particular direction or even toward a country not involved in the conflict and can lead to significant economic and political consequences. These flows can potentially cause a humanitarian catastrophe in the region and significantly affect the course of hostilities.

Recommendations

The Russia-Ukraine war has shown us the importance of **international cooperation** and partner relationships. These relations have a giant impact on local conflicts and modern warfare. The Ukrainian Armed Forces appreciate international military help and all efforts from democratic nations supporting us in this fight for our land, liberty, and democratic values of the world. We fully understand that without this help from our partners and friends abroad, it could not be possible for Ukraine to destroy the Russian war machine. Only with international support, we can grind the second-world army in Ukraine. On the other hand, our partners have a great source of knowledge and practical examples of how to prevent hybrid threads, and how to fight under their influence in Modern international security situations.

The military formations of democratic countries are potentially vulnerable to the means of hybrid warfare, as liberal democracies are structurally susceptible to the imperfections of laws and the influence of social and political actors. Countries should **improve the legislation** on the powers and protection of the armed forces and other power structures to counter the implicit threats of hybrid warfare. The development of scientifically based recommendations for increasing the effectiveness of countering hybrid threats during the preparation and conduct of an operation is an urgent and priority task of military science. Studying and predicting is extremely important to protect task forces. We should equip our commanders with effective tools to prevent or mitigate the impact of hybrid threats on the troops and accomplish their missions with minimum losses in soldiers and civilian populations. We should prepare national troops for Modern Warfare through the acquisition of **relevant capabilities** to respond to threats or “gray zone” and equipping them with capable task forces and trained commanders of all levels, developing sufficient doctrines, plans, manuals, and instructions.

The national security strategy of countries should mean that corruption is a fundamental threat. So, **zero tolerance for corruption should be the norm**. The situation when civil servants abuse their power reduces the country's defense capability and reduces public trust in state institutions, including the armed forces. The anti-corruption strategy must respond to the uniqueness of corruption threats to the country's security. Success on the battlefield in conditions of total war increasingly depends not only on the armed forces, but also on the cooperation of all state and non-state institutions. The priority direction of increasing resistance to implicit threats of

hybrid warfare is deepening **cooperation with other power structures**, the national police, customs service, border service, emergency services and others.

The democratic population of modern states is fertile ground for the information operations of the aggressor country to influence the mass perception or non-perception of certain events. Through the coordinated manipulation of facts in the information domain (*media, internet sources, rumors, and other tools*), the aggressor country can create a distorted virtual reality of the "gray zone" that affects perception and replaces real, substantiated truth with fiction. The main tasks of **active information defense** are anticipation of information influences on the population, information support of events in online modes, and immediate response to the facts of false accusations and slander. In the digital age, maintaining good **informational hygiene** is crucial for military personnel. We should train troops to critically evaluate, responsibly consume and thoughtfully share information to protect themself and others from manipulation, misinformation and information overload. Comprehensive Informational support of Decision-Making will help the population and troops to form a more accurate understanding of events, free from manipulation and contribute to a more informed and resilient society. Close cooperation with allies and partners, determination of high standards for the protection of critical infrastructure, improvement of cyber resilience, and creation of collective capabilities for rapid response to cyber-attacks are priority directions for **Cyber Defense**. In the face of the destructive power of cyberattacks by criminals, it is important to support initiatives to increase cooperation between law enforcement agencies, remove shelter from cyber criminals, and counter the illegal use of cryptocurrency to launder the proceeds of cybercrime.

Conclusion

The current state of international and national security shows that the use of hybrid methods of influence by an adversary can significantly intensify the crisis in a country and increase internal disputes. Hybrid tools of warfare decrease national defense capability and task force readiness in the theater of operations. Additionally, the use of such methods shapes both the strategic and operational environment of future operations. Countries seeking to enhance their global and regional influence will attempt to advance their foreign policies through the following strategies: dominance through non-military means, control in the information sphere, conducting military activities without declaring war or martial law, and utilizing proxy forces and criminal elements.

The experience of the Russian Federation's use of hybrid actions in Ukraine demonstrates that these tools have proven to be successful and relatively inexpensive. These two facts give

opponents of democratic countries no reason to cease using them. Moreover, the national Armed Forces of democratic countries are potentially vulnerable to hybrid warfare methods, as liberal democracies are structurally vulnerable to legal imperfections, the influence of social and political actors, false accusations, and cyberattacks. The notion that the asymmetric nature of hybrid actions is the weapon employed by a weaker adversary against a party with significantly greater military, technological, and human potential has evolved over time. As well as the notion that they are used mainly by non-state actors against the national state. This idea began under the influence of the "war on terror" concept and was further developed in the concept of hybrid warfare. Modern conflicts indicate that hybrid threats are becoming inter-state in nature and can even be employed by nuclear states. In cases where the aggressor country does not dominate in economic and military potential, the balance of power between the aggressor and the target of aggression shifts significantly in favor of a more flexible and multidimensional hybrid strategy.

References

Liang, Q., & Xiangsui, W. (1999). *Unrestricted warfare*. People's Liberation Army Literature and Arts Publishing House. https://www.c4i.org/unrestricted.pdf

Gerasimov, V. (2013). *The value of science in foresight*. Military-Industrial Courier. https://vpk-news.ru/articles/14632

United States Army Special Operations Command. (2015). *"Little green men": A primer on modern Russian unconventional warfare, Ukraine 2013–2014*. https://www.jhuapl.edu/Content/documents/ARIS_LittleGreenMen.pdf

Koval, M., Ivashchenko, A., Telelym, V., Sæther, T., Fedianovych, D., Uvarova, T., Hordiichuk, V., Andriianova, N., Peredrii, O., Shpura, M., & Ilch, V. (2023, December). *Theoretical and applied aspects of the Russian-Ukrainian war: Hybrid aggression and national resilience* [Monograph]. PC Technology Center. https://ideas.repec.org/b/tec/monogr/978-617-8360-00-9.html

Hoffman, F. G. (2007). *Conflict in the 21st century: The rise of hybrid war.* Arlington, VA: Potomac Institute for Policy Studies. https://potomacinstitute.us/reports/19-reports/1163-conflict-in-the-21st-century-the-rise-of-hybrid-wars

NATO StratCom COE. (2015). *Analysis of Russia's Information Campaign against Ukraine*. NATO Strategic Communications Centre of Excellence. https://stratcomcoe.org/publications/analysis-of-russias-information-campaign-against-ukraine/151

Chivvis, C. S. (2017). *Understanding Russian "hybrid warfare": And what can be done about it*. RAND Corporation. https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT468/RAND_CT468.pdf

Heickerö, R. (2010). *Emerging cyber threats and Russian views on information warfare and information operations* (Report No. FOI-R–2970—SE). Stockholm: FOI, Swedish Defence Research Agency. https://www.foi.se/rest-api/report/FOI-R–2970–SE.

Wetoszka, A. (2016). *An attempt to identify hybrid conflict*. Sõjateadlane, 2, 54–75. https://ojs.utlib.ee/index.php/st/article/view/23971

Cullen, P. J., & Reichborn-Kjennerud, E. (2017). *Understanding Hybrid Warfare. Multinational Capability Development Campaign* (MCDC): Countering Hybrid Warfare Project.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf.
Theohary, C. A. (2018). *Information warfare: Issues for congress* (CRS Report No. R45142), Version 5 Updated. Washington, DC: Congressional Research Service. https://crsreports.congress.gov/product/pdf/R/R45142/5.
Marsili, M. (2021).*The Russian Influence Strategy in Its Contested Neighbourhood*. In: Mölder, H., Sazonov, V., Chochia, A., Kerikmäe, T. (eds) The Russian Federation in Global Knowledge Warfare. Contributions to International Relations. Springer, Cham. https://doi.org/10.1007/978-3-030-73955-3_8
White House. (2022). *National security strategy*. The White House. https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf
Department of the Army. (2003). *FM 3-05.301: Psychological operations tactics, techniques, and procedures*. Headquarters, Department of the Army. https://fas.org/irp/doddir/army/fm3-05-301.pdf
National Academy of the Security Service of Ukraine. (2021). *Strategic communications in the conditions of hybrid warfare: A view from a volunteer to a scientist*. https://ekmair.ukma.edu.ua/bitstreams/4620ab20-66b3-4388-83f8-0d0b014bba3f/download
Bishop, M., & Goldman, E. O. (2003). *The strategy and tactics of information warfare.* Contemporary Security Policy, 24, 113–139. 121 https://www.tandfonline.com/doi/abs/10.1080/13523260312331271839
Horbulin, V. P., Dodonov, O. G., & Lande, D. V. (2009). *Information operations and public security: Threats, countermeasures, modeling*. Intertekhnologiya. https://sts.nangu.edu.ua/article/view/309909
TASS.(2022). "*Lavrov slams all-out sanctions spree, says West's values 'aren't worth a red cent"*. https://tass.com/politics/1427557
Braun, K. (2025). "*Ukraine's once booming grain industry..."* Reuters. https://www.reuters.com/markets/commodities/ukraines-once-booming-grain-industry-teetering-being-war-casualty-braun-2025-04-23/
INFORMS. (2025). " New Study Shows How Ukraine War Impacts Global Food Supply Chain, Urges Alternative Routes for Grains." https://www.informs.org/News-Room/INFORMS-Releases/News-Releases/New-Study-Shows-How-Ukraine-War-Impacts-Global-Food-Supply-Chain-Urges-Alternative-Routes-for-Grains
Dodd, E and Welsh, C .(2024): " Fracturing Solidarity: The Grain Trade Dispute between Ukraine and the European Union.." CSIS https://www.csis.org/analysis/fracturing-solidarity-grain-trade-dispute-between-ukraine-and-european-union
Scheuerman, K.A. (2023). *Weaponizing Wheat: How Strategic Competition With Russia Could Threaten American Food Security* National Defense University Press .The premier professional military and academic publishing house News. https://ndupress.ndu.edu/Media/News/News-Article-View/Article/3569549/weaponizing-wheat-how-strategic-competition-with-russia-could-threaten-american/
Zanuda, A. (2024). Why do Poles block Ukrainian border. *BBC News Ukrainian*. https://www.bbc.com/ukrainian/articles/cx7lxxw45w2o
Russell, M. (2021). *Russia's armed forces: Defence capabilities and policy*. European Parliamentary Research Service. https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689370/EPRS_BRI(2021)689370_EN.pdf
Congressional Research Service. (2024). *Russia's Wagner Private Military Company (PMC)*. https://crsreports.congress.gov/product/pdf/IF/IF12344

Marsili M. (2022). *Hybrid warfare: above or below the threshold of armed conflict*? Hungarian Defense Review 2022, Nr. 1–2, 36-48. https://iris.unive.it/retrieve/515f549b-56f5-4ab1-bf99-832b6feb77e0/Hungarian%20Defence%20Review%20150(1-2)%2036%E2%80%9348%2007_Marco+Marsili.pdf

Von der Leyen, U. (2021). *Statement by President von der Leyen on the situation at the border between Poland and Belarus*. Statement/21/5867. European Commission. Nov. 8, 2021. https://ec.europa.eu/commission/press corner/detail/en/statement_21_5867

Chapter 8: Do Drones Dream of Transparent Battlefields? Dealing with Past and Future Alternatives to the Tactical Crisis in Contemporary Warfare

Dr. Sandro **Teixeira Moita**, ORCID: https://orcid.org/0000-0003-4795-3880

Abstract:

The objective of this chapter is to provide a reflective analysis on the contemporary battlefield, with a particular focus on the emergence of novel tactical challenges. These challenges are precipitated by the evolution of technological capabilities, notably the integration of unmanned aerial vehicles (UAVs) and systems that facilitate real-time observation of combat operations. A review of recent conflicts, including the war in Ukraine and Israeli operations in the Gaza Strip, indicates that military forces with a high degree of tactical proficiency, armed with advanced systems, are encountering challenges in coping with the crisis. In light of these observations, this study proposes a systematic approach to understanding and addressing the crisis, leveraging the convergence of past and future technologies to shape the character of combat in the 21st century. One potential solution to the current impasse lies in the integration and combination of infantry, tanks, artillery, and drones. While this approach may entail significant political costs and profound societal changes, it is imperative to recognize that the consequences of military failure could be even more substantial. Consequently, investing in measures to address this crisis becomes imperative for Western powers and the countries whose doctrines are strongly influenced by them.

Keywords: Unmanned Aerial Vehicles, Drones, Emerging Technology

Introduction

The Russian-Ukrainian conflict that began on February 24, 2022 is the biggest conventional conflict on European soil since the Second World War (1939-1945). The scale of the actions that opened hostilities signaled the character of the conflict but were disregarded by both sides. The first weeks of the war, which were dramatic for Ukraine, were all about mounting a defensive action capable of stopping the Russian advances which, seen from a map, represented the Russian ambition to swiftly strike the Ukrainians with one blow, paralyzing the command center and consummating the fall of the local government, in a maneuver reminiscent of Soviet interventions in Warsaw Pact countries, such as Hungary in 1956 and Czechoslovakia in 1968. The Russians had prepared to achieve the submission of Ukraine through this coup, but their means were insufficient to do so (Zabrodskyi et al., 2022).

However, their contempt for the Ukrainians cost the Russians dearly: while the Russians had imagined swift and decisive action, the Ukrainians had decided to once again, as at other times in their history, to fight with the Russians. Thus, the predictions about how the operations would unfold were contradicted by reality. The absence of air superiority and the conduct of the first 48 hours of hostilities by the Russians are some of the elements that indicate the different nature of this conflict from other large-scale conflicts in history (Kofman, 2024).

Various reasons can be given for Russia's failure to achieve its objectives in the first three days of the conflict, including failures in tactical, operational and strategic aspects, with Russian deficiencies in command and control, as well as very serious logistical problems during the invasion (Zabrodskyi et al., 2022). But perhaps here it is worth remembering the political nature of war, as described by Clausewitz. Without this, it becomes impossible to understand the phenomenon of war, and by extension the Russo-Ukrainian war itself and the Russian failure to determine the effort required to achieve its objectives at the beginning of the struggle (Clausewitz, 1989).

However, the Ukrainian commitment to resistance, driven by political issues and a strong sense of identity, cannot be underestimated, and this has paid dividends, since it managed to stop the implementation of the Russian plan; just as the invaders did not act against the country's infrastructure at first, since they saw it as necessary for the occupation of the country. The speed required for the Russian advance was stopped on all axis of attack by the Ukrainians, by a set of regular and irregular units reacting to the passage of the troops and stopping them wherever they were (Zabrodskyi et al., 2022).

In order to understand part of the Russian failure in the first phase of the campaign, and the friction that followed from then on, it is necessary to understand a dynamic that the Russian-Ukrainian conflict has exacerbated on the battlefields of the 21st century: the tactical use of drones has changed the characteristics of combat, even influencing the use of troops and changing the correlation of casualties by equipment. As this chapter is being written, as of April of 2025, it is estimated that 75% of Russian combat casualties are inflicted by drone action (Brown, 2025).

In the Ukrainian case, the figures are similar, but in some cases, they exceed the Russian ones, reaching 80% (Santora et al., 2025), which undoubtedly demonstrates the transformation of combat in this war, from Ukrainian ambushes against Russian armored columns to attempts to overcome the trench stalemate in the Donbass by other means.

This chapter seeks to reflect on the possibilities for adapting infantry and armored vehicles to the use of drones in Ukraine and how these lessons, although preliminary, have been absorbed

in other conflicts, such as the fighting between the Israel Defense Forces and terrorist actors in Gaza, northern Israel and southern Lebanon.

The Transparent Battlefield

If before, the tactical crisis was represented by the challenge of dealing with the trenches of 1914 on the Western Front, now it appears in a different way. Just as in 1914, the increase in firepower destroyed conceptions as soon as the European armies clashed, now the presence of drones in the tactical field creates an impediment similar to the impossibility of outflanking an opponent in 1914.

The density of Russian and Ukrainian forces in the conflict is, from a historical point of view, is minimum, due to the size of the combat forces and the size of the front, which is more than a thousand kilometers long. In addition, the presence of fleets of drones in the air generates a visualization cycle that makes it very difficult for a force to move around the battlefield undetected, and once detected, it becomes the target of a firing suite fed by what can already be called a "reconnaissance-attack complex" (Noorman, 2024).

The transparency of the battlefield takes the idea that *'if it can be seen, it can be shot and destroyed'* to the extreme. In fact, the formation of a "reconnaissance-attack complex" or a "reconnaissance-fire complex" has been part of an evolutionary process of military technology since the 1980s, but with the presence of tiny processors and the popularization of drones, observation of the battlefield has become constant, and so maneuvering units involves a risk of detection and consequently suffering casualties before taking action (Noorman, 2024).

Visualization not only impairs maneuverability, it indicates the need for an entire reorganization of a fighting force, since the presence of sensors combined with drones leads to the expansion of attack possibilities, since logistical tails and command centers can be attacked with precision, making offensive action vulnerable, making it difficult to command and control operations and even how to sustain them (Noorman, 2024).

The Russians and Ukrainians have been using drones at different levels of the war, from the tactical to the strategic. The applications at the strategic and operational levels have mixed effects and are not capable of being a miracle weapon that could change the course of the war, especially for the Ukrainians. However, at the tactical level, the use of drones has changed the shape of combat and the use of units, as well as creating significant psychological effects, not only on combatants, but also with the proliferation of records of their use on the internet (Lushenko, 2024).

The use of drones on a large scale, combined with the effects of permanent observation of the battlefield, has led to the perception of their transparency, where any movement is detectable and thus actions are taken to attack a moving force. Beyond this, the proliferation of drones also seems to be, in the minds of political leaders, a way of offsetting issues of troop recruitment or even maximizing firepower (Lushenko, 2024).

This leads to the formation of large fleets or constellations of drones, which requires greater management, increasing the need for command-and-control platforms in order to achieve greater effectiveness and damage to the adversary. Swarms of drones are a new reality, even more so with the use of artificial intelligence (AI), which coordinates the actions of dozens and hundreds of drones and loitering munitions. The Russians have made use of this in Ukraine to attack positions on the front lines as well as cities (King, 2024).

The massive presence of drones takes the issue of observation to new levels. More than 86% of targets taken out by the Ukrainians are drones, with hundreds of them meeting and clashing in the skies over Ukraine (Kunertova, 2023). The accuracy of artillery has been greatly improved by the images provided by drones, which can calculate, observe, fire and correct the shot in a matter of minutes, a process that without them would take more than half an hour or more (Kunertova, 2023).

Contrary to what was imagined, the war in Ukraine did not turn into a war of sophisticated drones with great attack capabilities, as was used by the United States in the War on Terror campaigns. This was due to friction, involving anti-aircraft defense, electronic warfare and cybernetic means, which forced both sides to take the path of adaptation in combat, leading to an explosion in the use of FPV (first-person view) drones, something unexpected by experts and the military (Kunertova, 2023). Possible reasons for the adoption of such systems are their wide availability on the market, the adaptability of the use of such drones to turn them into ammunition and the simplicity of training pilots and navigators.

There are various reasons why the Ukrainians and Russians have set about adapting FPV drones for war. In addition to their low cost and ease of operation, their action puts fewer troops at risk, apart from the difficulties of detection as they fly at low altitude and contain materials such as rubber or cardboard, to name a few. Although drones from military industries such as the American Switchblade 300 and 600, the Russian Lancet and even KUB-BLA drone systems are effective, FPV drones armed with artillery or personal grenades in kamikaze-type missions have caused heavy casualties (Kunertova, 2023).

Another element affected by the continuous observation of the battlefield by drones is initiative, which is vital for conducting operations. Commanders tempted by the accelerated flow

of information in real time tend to want to redo plans and change orders, something that can cause a loss of initiative, especially in offensive operations (Watling, 2024).

Here, it is a matter of understanding that although technology has evolved, the command structure still operates at intervals, which leads to the need to adapt to the reality of continuous observation. Deciding whether or not to respond to an action can now be an extremely crucial decision, since the adversary may be waiting for something to reveal the disposition of forces and thus attack them when revealed (Watling, 2024).

The application of drones from a tactical perspective

The Russian-Ukrainian conflict shows us that the most successful level in the application of drones has not been operational or strategic, but tactical. So, it's worth understanding why, at least in the tactical field, drones have been a transformative element, especially in the employment of platoons and companies. With low-cost drones in the hundreds of dollars, operators on both sides have adapted commercial FPV-type drones to be low-cost versions of loitering munitions, increasing firepower in the hands of small units (Kunertova, 2025).

Before dealing with the issue of the use of drones, it is important to clarify the difference between the levels of war: strategic, operational and tactical. This differentiation is more common in Western military thinking, but it is not exclusive. The strategic level is linked to the political decision to use force and how this will be translated into military purpose, which leads us to the operational level, responsible for conducting military campaigns and major operations that make war, which leads us to the combat dimension, at the tactical level, where battles, engagements and actions of small units take place (Harvey, 2021).

In order to understand the success of the use of drones at the tactical level, we need to look at the question of adaptation. With a drone race on both sides, it can be seen that the evolution of the dynamics of their use in combat follows a logic with two main elements: firstly, their use generates countermeasures of different kinds, such as small arms fire, electromagnetic interference and even cyber actions; secondly, the availability of mechanical and electronic components that allow for maintenance or facilitate changes in drone design (DeVore, 2023).

The use of drones by platoons and companies in combat also changes the character of combat, since it increases the situational awareness of soldiers in the fight and thus drones have become as vital as ammunition and artillery shells. Drones are also tools available to wear down and exhaust an adversary by forcing the adversary to expend valuable anti-air missiles or other expensive anti-drone countermeasures. Due to the observation capabilities they bring, they can

lighten the logistical footprint, as attacks become more precise, reducing the amount of ammunition used against a target (Kunertova, 2023).

It is important to say that although drones represent a transformation on the battlefield, they have not become the decisive factor. Tanks, armored personnel carriers, and infantry fighting vehicles have an important role to play, as well as artillery. Drones have not changed the relevance of these systems, and in fact can even serve as amplifiers of the combat capabilities of both tanks and artillery. Although the start of the war, with Russian armored columns being decimated by the action of anti-tank missiles and drones, created a false perception of the obsolescence of the tank in 21st century warfare, there is clearly still a role for it on the battlefield (Lee, 2022).

In fact, when you look at the action of drones against tanks, for example, you realize that there are very few cases in which the use of an FPV drone with ammunition acting as a *kamikaze* is successful. Apart from targeting the tank's most vulnerable areas, such as its rear, or the top opening hatch, the drone has often been the instrument that has slowed down the tank, and combined with missiles or artillery, has helped to destroy it (Pettyjohn, 2024).

The use of drones has led to a change in the way platoons and companies deploy on the battlefield, as well as tanks and armored vehicles. As of 2023, it is clear that the infantry is operating with many more drones, not only for attack, but also to coordinate their own actions, with combat being conducted less with the presence of armored vehicles and more in a dismounted manner, on foot (Pettyjohn, 2024).

Foot combat, due to the constant presence of drones in the attack and observation roles, has also led to a phenomenon: dispersal of forces, something that would have been unthinkable in previous campaigns, where the concentration of units was always an indicator of the intensity of effort, whether offensive or defensive, and its chances of success. Now, Ukrainian brigades are deployed in sectors of the front that are much larger than what is expected in NATO-type doctrine armies. One Ukrainian brigade, for example, was responsible for defending 27 kilometers of front with just four battalions (Watling & Reynolds, 2025).

This spacing is due to the permanent threat posed by drones. Reducing the density of forces, something unthinkable in military doctrine a few years ago, is now a reality in the trenches of Ukraine. Concentration is only possible if the unit has the ability to use decoys, conceal the use of terrain and have reversal positions to which they can relocate in the event of an attack. Dispersal is not only on the front line, but also in the depth that the units have come to cover. A Ukrainian infantry company goes an average of three kilometers deeper, while a battalion goes seven (Watling & Reynolds, 2025).

With adaptations like this, combat itself also ends up getting deeper. Tanks and armored vehicles are reserved for decisive moments, coming out of their hidden positions to support an action with their firepower and thus support assaults or break up enemy attacks, returning to their shelters before being attacked by the opposing reconnaissance-fire complex. It should be remembered that while the Russians have always had a large tank presence even in non-armored units, the Ukrainians are dedicating a tank company or battalion to each brigade (Watling & Reynolds, 2025).

The Challenge - *Breaking the Stalemate and Building Capacity on a New Battlefield*

How can we deal with the impasse of the tactical crisis on the battlefields of the 21st century? One possibility would be greater integration between tanks, artillery, infantry and drones, something that is already being observed both in Ukraine and in Israel Defense Forces' [IDF] operations in the Gaza Strip, northern Israel and southern Lebanon after the terrorist attacks of October 7, 2023.

To this end, it is necessary to consider the dimensions of electronic warfare and its effects on the electromagnetic spectrum, since the effects of these conflicts are likely to be replicated in others in the near future. Also to be considered are the operating limitations of the drones themselves, as in the case of FPVs, because they are guided by radio frequency, end up creating obstacles to concentration because one drone can interfere with the guidance system of another. This helps explain why, for example, between 60% and 80% of Ukrainian FPVs launched in combat fail to hit their targets (Watling & Reynolds, 2025). Pilot skills, the situation at the front and electronic warfare help explain these figures (Watling & Reynolds, 2025).

An interesting example of how such integration can work is a lesson in urban combat that the IDF learned from the war in Ukraine. The presence of drones on the battlefield, and the fact that they can observe at different heights with great speed, reduced the presence of adversaries beyond the second level of a building, since they could be detected quickly and attacked with artillery or aviation fire (Watling & Reynolds, 2024).

Drones were also needed to better guide IDF units in their advance through Gaza, since with the use of heavy firepower, artillery and aviation, many of the roads were littered with ruins and craters, causing the loss of vehicles that overturned on such obstacles. They also served as tools for troops to coordinate requests for artillery and aviation support, helping to translate map points into visual references (Watling & Reynolds, 2024).

The ability to observe areas of operation of terrorist groups such as *Hamas* and *Hezbollah*, among others, is something that has been refined by Israel for many years, but not in the tactical

dimension, since many of the drones used for such observation were large, while when the war broke out, the IDF became very concerned about the presence of drones launched by these and other groups against Israeli territory. It wasn't just Israelis who had seen videos of the war in Ukraine.[1]

In fact, Israeli operations in Northern Israel and southern Lebanon witnessed *Hezbollah*'s use of drones against Israeli targets to such an extent that electronic warfare resources had to be used to interfere with and degrade the terrorist group's operational capabilities against the IDF. Israeli capabilities in the electromagnetic spectrum were such that the IDF troops themselves in operations reverted to using printed maps rather than digital interfaces.[2]

The use of drones also had an impact on the operations planning cycle, since, when fighting irregular forces, Israel had to identify its targets in order to be able to carry out attacks legitimately, and thus not lose its freedom of action or have it restricted. Continuous observation allowed for the deconfliction of fire support as well as the confirmation of elements that would make the mission impossible, such as the presence of civilians, collateral damage and other sensitive issues.[3]

Both in the case of Israel,[4] and in the case of the Russian-Ukrainian conflict, the tactical use of drones is a process that is ahead of doctrine, which has caused problems for the troops. With insufficient training because of lack of training doctrine, lack of manuals and appropriate techniques, it has become necessary for soldiers to learn in real conditions, as well as to learn how to defend themselves against opposing tactical drones. The need to operate drones means that each Ukrainian assault group has an equal number of pilots supporting it, which shows the growing option for using drones, even at the cost of manpower (Pettyjohn, 2024).

A look at military history shows that the first attempt to break out of a tactical crisis, such as that imposed by the First World War (1914-1918), was at Cambrai in 1917. As in the French camps, the attempt to break through necessarily involved greater coordination of systems and men. Despite the predictions of autonomous weapons guided by artificial intelligence systems in many recent military and academic texts, this clashes with the reality of what we see in Ukraine: groups or “packs” of drones operating rather than the large hordes or swarms conceived by specialists (Pettyjohn, 2024).

The fact is that the Russian-Ukrainian conflict, being the first large-scale and intense drone war, will play a decisive role in how we think about the absorption of tactical drones into military doctrine. It will be a process with varying perceptions, since the rapid adoption of commercial

[1] Author's interview with IDF brigade officers, February 2025.
[2] Author's interview with IDF officers at the Alma Research and Education Center, February 2025.
[3] Author's interview with IDF officers at the IDF Spokesperson's Unit, February 2025.
[4] Author's interview with IDF brigade officers, February 2025.

platforms was due to the need for combat and because military supply chains were unable to provide the mass needed for combat. As we can see, this is not something that drastically changes warfare, but rather influences its course and in this battle, adaptation is the key, as it regulates the transformation of armored and infantry forces in modern combat (DeVore, 2023).

One way of thinking about integration and a possible model is through the role of a robust infantry, not only by operating more drones, but also by mechanization, since although the detection footprint of an infantry company is smaller than that of a mechanized company, the advantages offered by armored protection are too important to be overlooked. The operations in Ukraine and Gaza show the combative power of infantry supported by armored vehicles with drones and how this multiplies their firepower as well as that of support, such as artillery and aviation.

Part of the integration between drones, infantry, tanks and artillery involves a certain revision of how we understand the roles of each in combat. As stated above, a robust infantry will be equipped with greater firepower but also with greater support in terms of providing more accurate data to artillery and aviation, by means of drones. Strengthening the infantry also means equipping it with systems that can detect, degrade and destroy adversary drones in operation, in order to preserve its freedom of action on the ground.

Thinking about how drones can be integrated into military formations is not an easy task. But faced with a scenario in which this technology is becoming more widespread and increasingly cheaper, it is imperative to consider a reasonable model for how tactical drones can be used on battlefields. This will serve as a model for the phenomenon of robotization and autonomous systems, but it involves a new vision of how to design combined arms, as in the tactical crisis of 1914.

Designing this integration at the most tactical levels is a real challenge, but one that can be tackled. Dispersion, firepower and continuous observation are elements of the transparent battlefield, which are in the way of the new operational concepts of various Western armies, such as convergence operations.

In these new concepts, tactical units will be even more demanding in terms of operational and combat capabilities, combined with other capabilities such as electromagnetic emissions, decoy measures and other non-kinetic measures, in a multi-domain operating scenario (Segal, 2023). In fact, to think of such a model of integration between drones, infantry and armor is to exercise in practice what convergence prescribes, but it remains to be seen how Western militaries will process such changes.

Conclusion - ***Drones Experiencing the Dream of the Transparent Battlefield***

Clausewitz reminds us that the enemy is a living force, and therefore reacts (Clausewitz, 1989) and it is in this spirit that this chapter has sought to understand the tactical dynamics of the application of drones, especially FPV drones, on battlefields and what this means for combat in the 21st century. Although at first glance it appears to be a revolution, what we see is a great circus of adaptation, common to the very dynamics of war as a phenomenon.

Small-capacity, tactical drones are here to stay on the horizon of 21st century warfare. Their price, availability and ease of operation make them extremely attractive not to be used. Their popularity, especially when we think of FPV drones, brings yet another feature, which is that soldiers may already have knowledge of their operation in their civilian lives before joining the Armed Forces, something that reduces costs and speeds up the cycle of use of such technologies.

Verticality and dispersion, traits observed in the behavior of the infantry, are direct results of the application of drones on the battlefield, which has been transformed by the capabilities of continuous observation at different levels of height and visualization, even at night or beyond camouflage by thermal means. Tactically, the impact of drones has even changed the psychology of the troops, because now the most feared sound is no longer that of an artillery salvo or the engine of a tank, but the sound of the rotors of an FPV drone.

Therefore, thinking about the application of drones and integrating them into a system that considers maneuver, and assault seems to be the only way to overcome the impasse represented by the tactical crisis seen in Ukraine. If we are already talking about the reconnaissance-attack complex and the reconnaissance-fire complex, the time has come to think in the tactical field, in a more systemic way, about a maneuver and assault complex, with drones integrated with tanks, infantry and artillery.

Reflecting on how to integrate drones into the tactical field is necessary in order to think about force designs in the 21st century and the manifestation of combat, since, with the popularization of such technologies, their greater accessibility tends to reverberate beyond the battlefields. It should be considered that not only armies are observing the lessons from Ukraine. For example, beyond the sphere of war: in security, criminal and terrorist groups can acquire such technologies and use them against police forces, just as *Hamas* and *Hizballah* use them against the IDF in combat.

In short, if drones dream of a transparent battlefield, it's important to understand the dynamics and functioning of their application at various levels, such as tactical, operational and strategic. By understanding this, you can escape a trap and build a way out, so that this dream doesn't become a costly nightmare.

References

Brown, S. (2025, March, 28). Casualty Figures Reveal Game-Changing Impact of Drones on Ukrainian Battlefield. *Kyiv Post*. https://www.kyivpost.com/analysis/49712.

Clausewitz, C. (1989). On War. In *On War*. Princeton University Press.

DeVore (2023). "No end of a lesson:" observations from the first high-intensity drone war. *Defense & Security Analysis*, 39:2, 263-266, DOI: 10.1080/14751798.2023.2178571

Harvey, A. S. (2021). The levels of war as levels of analysis. *Military Review*, 99(6), 75-81.

King, A. (2024): Robot wars: Autonomous drone swarms and the battlefield of the future, *Journal of Strategic Studies*, DOI: 10.1080/01402390.2024.2302585

Kofman, M. (2024). The Russia-Ukraine War: Military Operations and Battlefield Dynamics. In: Brands, H. (editor) 2024. *War in Ukraine: conflict, strategy, and the return of a fractured world.* Johns Hopkins University Press.

Kunertova (2023). Drones have boots: Learning from Russia's war in Ukraine. *Contemporary Security Policy*, 44:4, 576-591, DOI: 10.1080/13523260.2023.2262792.

Kunertova, D. (2025). Learning the Right Lessons: How Ukraine Has Changed Drone Warfare. *Warfare and International Relations*, 6.

Lee, R. (2022, September, 6). *The Tank Is Not Obsolete, and Other Observations About the Future of Combat.* War on the Rocks. https://warontherocks.com/2022/09/the-tank-is-not-obsolete-and-other-observations-about-the-future-of-combat/.

Lushenko, P. (2024, February, 16). Cult of the drone: At the two-year mark, UAVs have changed the face of war in Ukraine - but not outcomes. *The Conversation*. https://theconversation.com/cult-of-the-drone-at-the-two-year-mark-uavs-have-changed-the-face-of-war-in-ukraine-but-not-outcomes-221397.

Noorman, R. (2024, March, 27). *The Return of the Tactical Crisis*. Modern War Institute at West Point. https://mwi.westpoint.edu/the-return-of-the-tactical-crisis/

Pettyjohn, S. (2024, March, 5) *Drones are Transforming the Battlefield in Ukraine But in an Evolutionary Fashion.* War on the Rocks. https://warontherocks.com/2024/03/drones-are-transforming-the-battlefield-in-ukraine-but-in-an-evolutionary-fashion/.

Santora, M., Jakes, L., Kramer, A. E., Hernandez, M., & Sholudko, L. (2025, March 3). A Thousand Snipers in the Sky: The New War in Ukraine. *The New York Times.* https://www.nytimes.com/interactive/2025/03/03/world/europe/ukraine-russia-war-drones-deaths.html.

Segal, R. (2023). Who “does” MDO? what multi-domain operations will mean for-and require of-the army’s Tactical Units - Modern War Institute. Retrieved from https://mwi.westpoint.edu/who-does-mdo-what-multi-domain-operations-will-mean-for-and-require-of-the-armys-tactical-units/

Watling, J. (2024). *The Arms of the Future.* London: Royal United Services Institute for Defense and Security Studies.

Watling, J.; Reynolds, N. (2024). *Tactical Lessons from Israel Defense Forces Operations in Gaza, 2023*. London: Royal United Services Institute for Defense and Security Studies.

Watling, J.; Reynolds, N. (2025). *Tactical Developments During the Third Year of the Russo-Ukrainian War*. London: Royal United Services Institute for Defense and Security Studies.

Zabrodskyi, M., Watling, J., Danylyuk, O. V., & Reynolds, N. (2022). *Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine, February-July 2022*. London: Royal United Services Institute for Defense and Security Studies.

Chapter 9: Negotiation as a Key Enabler Behind Multi-Domain Operations

Pedro B. **Água**, ORCID: https://orcid.org/0000-0003-1886-9938
Vitor **Conceição**, ORCID: https://orcid.org/0000-0003-3689-9954
Anacleto **Correia,** ORCID: https://orcid.org/0000-0002-7248-4310

Abstract:

After decades without significant threats, the world is sensing a rise in the risk of major conflicts across various geographies. Multi-Domain Operations [MDO] is a systems concept and the latest concept from the North Atlantic Treaty Organization [NATO] to tackle the complexity inherent in the present-day defence paradigm and threats potentially impacting the millions of people the Alliance seeks to protect, along with the democratic and humanistic values that characterise Western society. MDO is not only a response to increased tensions but also to Emerging Disruptive Technologies [EDTs] in relation to those threats. Underneath and sustaining MDO, however, will be a fabric of systems arranged as part of a Systems-of-Systems [SoS], providing emergent capabilities that no isolated system possesses. A System-of-Systems may have multiple levels of stakeholders with possibly competing interests, perhaps contradictory objectives and purposes, and occasionally different operational priorities with no clear escalation routes. It may also have multiple lifecycles with elements being implemented asynchronously and multiple owners making independent resourcing decisions. This idea suggests that trust and agreement mechanisms shall be the essence behind lasting or periodic participation of a potential dynamic set of systems arranged as Systems-of-Systems. However, for such trust and agreement mechanisms to be effective, a dynamic approach must be at the core of the process – negotiation. This paper argues that negotiation as an organisational capability is a critical skill and a key enabler in achieving effective MDO, as the human component of such participating organisations, also known as subsystems, may be simultaneously the strongest and weakest link that MDO will rely on. The methodological approach followed in this paper is based on systems thinking approaches to problem-solving, and its goal is to provide insight into enabling factors without which MDO may fall short of expectations in a world perceived as dangerously advancing toward a new age of significant conflicts.

Keywords: Agreements, Multi-Domain Operations, Negotiation, Systems-of-Systems, Trust.

Introduction

Faced with a perceived increase in tension in the Western North Atlantic geography, the North Atlantic Treaty Organization [NATO] launched the Multi-Domain Operations [MDO] concept in May 2023 to enhance its deterrence capability (ACT, 2023).

It is accepted that history repeats itself, but never precisely in the same way. Current world conflicts differ significantly from past ones within a paradigm of unprecedented complexity, which demands new approaches and defence concepts that span from adapting organisational systems to full systems-of-systems arrangements. MDO will be comprised of such Systems-of-Systems [SoS] arrangements, a paradigm where traditional Command and Control [C2] will face challenges. Contrary to designed systems, Systems-of-Systems - composed of organisational systems that are rarely designed - are formed from existing systems that retain their managerial independence and governance, evolving independently of any centralised design, which makes C2 challenging. Organisational systems have challenges of their own, and the MDO concept NATO is pushing for, besides technologically engineered systems, will comprise of a considerable number of organisational systems. The human dimension, if not managed effectively, may jeopardise the intended effects or desired capabilities. Past experiences with concepts such as *joint domain operations,* including interoperability, have shown that technology and technological interfacing may not be the main problem. Human characteristics such as trust and agreement mechanisms at the organisational level – in short, negotiation, as an organisational capability– will be key for attaining an effective MDO paradigm. The motivation behind this research stems from the need to highlight the critical human dimension at the centre of MDO, a debate that is necessary to achieve the goal of improved deterrence and defence. MDO will demand the 'construct' or arrangement of distinct organisational typologies. At one side, there is the traditional military organisations; at the other, the need to interrelate with civilian organisations, both governmental and non-governmental, including private sector organisations, to attain the desirable convergence of effects.

Regardless of the broader MDO concept, this text focuses on military-civilian cooperation (Axelrod, 1984), which may prove to be one of the weakest links in the chain towards achieving a truly MDO paradigm. Such attainment may have many potential spheres of friction due to different organisational and ethnic cultures, and differing interest levels among military and non-military organisations.

Following this introduction, the subsequent section provides relevant background. The third section provides a brief overview of the used methodology. The fourth section provides some analysis results once the methodology has been applied. Section five concludes this text.

Multi-Domain Operations originates a new paradigm

Attaining the MDO paradigm across the Alliance demands an effort across many themes – operations, technology, organisation, and even political wisdom – and multiple domains in the field, which span beyond pure military organisations, to achieve a 'Total Defence' paradigm. It is becoming apparent that civil governmental entities as well as private sector actors will be part of the systems-of-systems arrangement that will help sustain MDO (Dailey, 2023):

> "orchestration of military activities, across all domains and environments, synchronised with non-military activities, to enable the Alliance to create converging effects at the speed of relevance."

Achieving the MDO is challenging, both at the technological, organisational, doctrinal, and educational dimensions, and perhaps at the agreement mechanisms dimension, where joint problem-solving, a collaborative approach to negotiation, is of the essence. Often, most of the effort has traditionally been placed in themes such as technology, interoperability standards, doctrine, and organisation, but has fallen short in some human dimensions.

Systems-of-Systems as the infrastructure underneath MDO

A pure technological and organisational integration view of MDO, several critical concepts include traditional military operations, interfacing and coordination with governments, defence industrial and technological bases [DTIB], Non-Governmental Organizations [NGOs], supply chains, support and logistics, and operations doctrine. Such domains may be complicated but not complex in comparison (Rihani, 2002; Weick & Sutcliffe, 2015). The diversity of technological systems and organisations required to achieve an MDO paradigm suggests that MDO will most likely be supported by collaborative and acknowledged Systems-of-Systems [SoS], which can be defined as "a system of interest whose elements are managerially and/or operationally independent systems" (Dahmann, 2015). "These interoperating and/or integrated collections of constituent systems usually produce results unachievable by the individual systems alone" (INCOSE, 2015, p.8). According to Dahmann (2015), SoS exhibit the following characteristics:

- *Operational Independence of Constituent Systems*. Constituent systems function independently of the SoS and other systems. These systems typically existed prior to the formation of the SoS to support a new capability.
- *Managerial Independence of Constituent Systems*. Systems within a SoS are managed independently, and their owners or managers may evolve them to meet their needs, regardless of the broader interest of the SoS.

- *Evolutionary Development Processes*. SoS development relies on developments in the integrating systems. Such developments may occur asynchronously based on the constituent systems' independent development processes and will. This makes the SoS development incrementally rather than designed as typically envisioned in engineered systems.
- *Emergent Behaviour.* Emergent system behaviour is a function of the interactions and relationships among system elements rather than the behaviour of individual elements. It emerges from a combination of the properties and behaviour of the system elements and the system's structure or allowable interactions between the elements. It may be triggered or influenced by a stimulus from the system's environment. (Emmeche, Koppe, & Stjernfelt, 1997).

In the MDO context, such SoS would include human/organisational systems, not technological ones. Such organisational systems may differ among allied member countries, where each country has several distinct organisational systems (*e.g., Navy, Army, Air Force*) with their own unique cultures. Moreover, when it comes to private sector actors, i.e. participating systems, it is easy to envision an almost limitless diversity of organisational profiles that must be integrated to support the MDO paradigm. Before advancing on the distinct organisational systems integration (military, governmental, and private sector), it is important to clarify some properties of *collaborative* and *acknowledged SoS,* which may raise constraints for the needed "arrangements" (*as opposed to other types of constituent systems, as the "directed" or even the "virtual" types*). According to Dahmann (2015):

> "In a collaborative SoS, the constituent systems interact voluntarily to comply with agreed-upon objectives."

As for an *acknowledged SoS*, the constituent systems recognise the overall objectives; have a designated manager, and have resources to contribute to the overall SoS construct. However, they keep their independence, ownership, funding, goals, self-development, and sustainment approaches. Any changes in the participating systems are based on agreements between the SoS and the individual acknowledged systems. Moreover, virtual systems lack a central management (and perhaps governance) authority and a centrally agreed-upon purpose. Virtual systems within a SoS rely on self-organising mechanisms to maintain them.

Finally, *directed SoS* are engineered and managed to fulfil specific purposes and are centrally managed. The constituent systems maintain their independence and autonomy yet are subordinated to the centrally managed purpose.

Differences between System-of-Systems "Engineering" and Systems Engineering are considerable (

Table **9.2:**) and have implications for achieving an MDO paradigm, as the supporting system of systems cannot be engineered in the traditional sense but "arranged" instead.

Table 9.2: *Differences between systems engineering and SoS "engineering"*

Systems tend to …	Systems of systems tend to …
▪ Have a clear set of stakeholders ▪ Have clear objectives and purpose ▪ Have clear operational priorities, with escalation to resolve priorities ▪ Have a single lifecycle ▪ Have clear ownership with the ability to move resources between elements	▪ Have multiple levels of stakeholders with mixed and possibly competing interests ▪ Have multiple, and possibly contradictory, objectives and purposes ▪ Have multiple, and sometimes different, operational priorities with no clear escalation routes ▪ Have multiple lifecycles with elements being implemented asynchronously ▪ Have multiple owners making independent resourcing decisions

Source: INCOSE. (2018). *Systems of Systems Primer*. International Council on Systems Engineering (INCOSE). Used with permission. © INCOSE. All rights reserved.

According to INCOSE (2018): "These differences are not as black and white as the table might suggest, and in each case, the degree of difference varies in practice. Modern systems tend to be highly inter-connected so that the assumptions that lead to the characteristics of Systems Engineering are less frequently met." (

Table **9.2:**).

This text focuses on a pre-conflict or preparation stage, where collaborative and acknowledged SoS typologies will most likely be the norm and where private sector participant systems decide to participate based on agreements dependent on incentive mechanisms. Such incentive mechanisms shall consider the nature, organisational cultures, and motivations of private sector entities, and negotiation and agreement mechanisms will be at the core of the SoS arrangement process.

Negotiation as a critical enabler for MDO

Experience suggests that technological systems are merely complicated but not as complex as human or organisational systems. Taking the well-known Pareto 80/20 principle, where

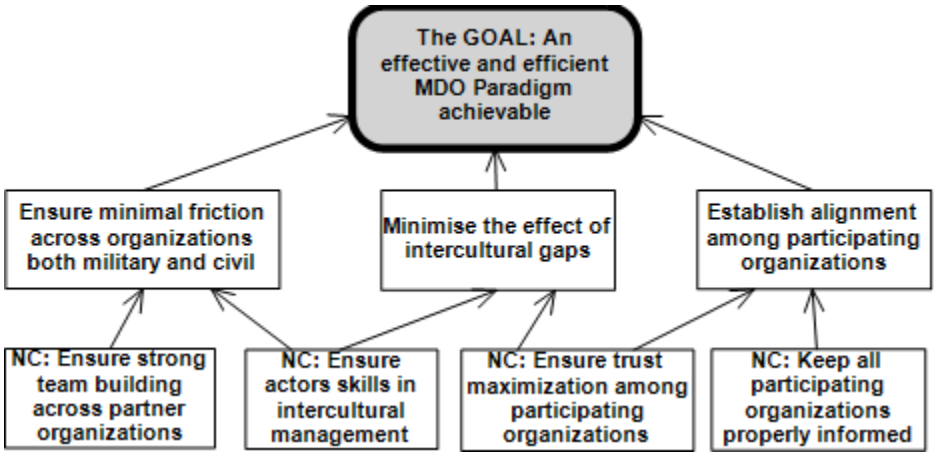
most effort should be placed on the most critical few causes of a given problem, why do most decision-makers keep placing the focus on technology as they are typically complicated, but not complex? The distinction between complicated and complex concepts is crucial, and David Snowden's *Cynefin* Framework offers clarity on such concepts (Snowden & Boone, 2007; Snowden & Rancati, 2022).

Accordingly, in a complicated context cause-and-effect mechanisms are more or less identifiable, while in a *complex context,* cause-and-effect relationships are not easily identified, as they may be distant in space and/or time. Additionally, experience across multi-organisational efforts suggests that complex contexts are those where the human dimension, sometimes political, may become the primary constraint. The human dimension in arranging a SoS to enable an MDO paradigm requires attention to the concept of negotiation, particularly complex negotiations involving multiple and culturally distinct parties, as a critical enabler for MDO that includes military and civil actors, particularly those from the private sector. Therefore, a note on negotiation, specifically multiparty negotiations, is due (Lewicki et al., 2007). Multiparty negotiations are among the most complex types, as it is difficult to clarify all party's interests and motivations; it is challenging to understand power imbalances, and it is a context where coalitions are common, which brings a further layer of complexity into the equation. It is clear that some analysis is due for understanding the current paradigm and what needs to be done to achieve a desirable future paradigm. A note on the following method, based on logics, is provided in the next section.

Enablers to achieve an effective MDO paradigm

To achieve an effective and efficient MDO paradigm, several Critical Success Factors [CSF] shall be in place. These are typically enabling conditions which maximise the chances of attaining the end objective. On their side, these CSFs also require the support of certain necessary conditions [NC] (Figure 1). For instance, to *Minimise the effect of intercultural gaps*, it is needed some NCs, such as *Ensure actors skills in intercultural management*, and ensure trust maximization among participating organizations.

Figure 9.1: *Critical Success Factors and Necessary Conditions for Achieving the Goal*



The Methodology –Theory of Constraints

The methodological approach used the Theory of Constraints [TOC] as a central framework for analysis and synthesis (Goldratt, 1990; Goldratt, 1992; Scheinkopf, 1999; Schragenheim, 1998; Dettmer, 2007). TOC employs a framework comprising distinct logic trees that collectively address four critical questions for any organisation when solving complex problems – those that are typically systemic (Table 2).

Table 9.3: *The TOC has four fundamental questions*

Key Questions	Objectives
Why change?	To pursue a desirable goal or new paradigm
What to Change?	What needs to change in order to eliminate undesirable effects [UDE]
What to Change To?	What do changes look like to achieve desirable effects? [DE]
How to cause the change?	What enabling conditions or prerequisites are needed to reach the desirable effects?

Source: (Dettmer, 2003)

Answering the first two questions (‘*Why change?’* and *‘What to change?’*) is related to the complex problem definition and the realisation of such a problem’s consequences if it is not adequately addressed. Firstly, the ‘Why change?’ question relates to the election of *the Goal* for the problem or *system of interest* [Sol]. In the present case, the goal may be stated as: ‘*an effective and efficient MDO Paradigm achievable’*. From its side, this goal implies management and leadership of complex operations that must be characterised accordingly. Secondly, the question ‘*What to change*?’ helps characterise the root causes underlying the visible symptoms in our

systems of interest, which in the case of MDO, may be a system-of-systems comprising many distinct organisations, both military and non-military.

Answering the last two questions *('What to change to?' and 'How to cause the change?'*) prompts one to design a solution to address the defined problem(s) by eliminating or mitigating the effects of the identified root causes behind undesirable effects, and how to deploy such a solution in practice with the intended net benefits. The Logical Thinking Process, central to Goldratt's Theory of Constraints (1990), underlies the methodological approach employed in this study, and it incorporates a specific tool for validating causality – the Categories of Legitimate Reservation, or CLR. The CLR are a set of eight questions that each causal relationship (represented by an arrow within the logic trees or diagrams), which ensure robustness and therefore, validity when the causal influence is compliant with all questions; that is, if any reservations are expressed by the application of any of the eight clauses, the causality may be at stake (Burns & Musa, 2001). However, the reservation clauses promote model improvements and do not necessarily remove causal relationships (Table 3). Dettmer (2003) provides a comprehensive explanation of the CLRs.

Table 9.4: *The Categories of Legitimate Reservation*

Clauses	
1. Clarity	5. Additional cause
2. Entity existence	6. Cause reversal
3. Causal Existence	7. Predicted effect
4. Causal insufficiency	8. Tautology

Source: (Adapted from Dettmer, 2003)

Results

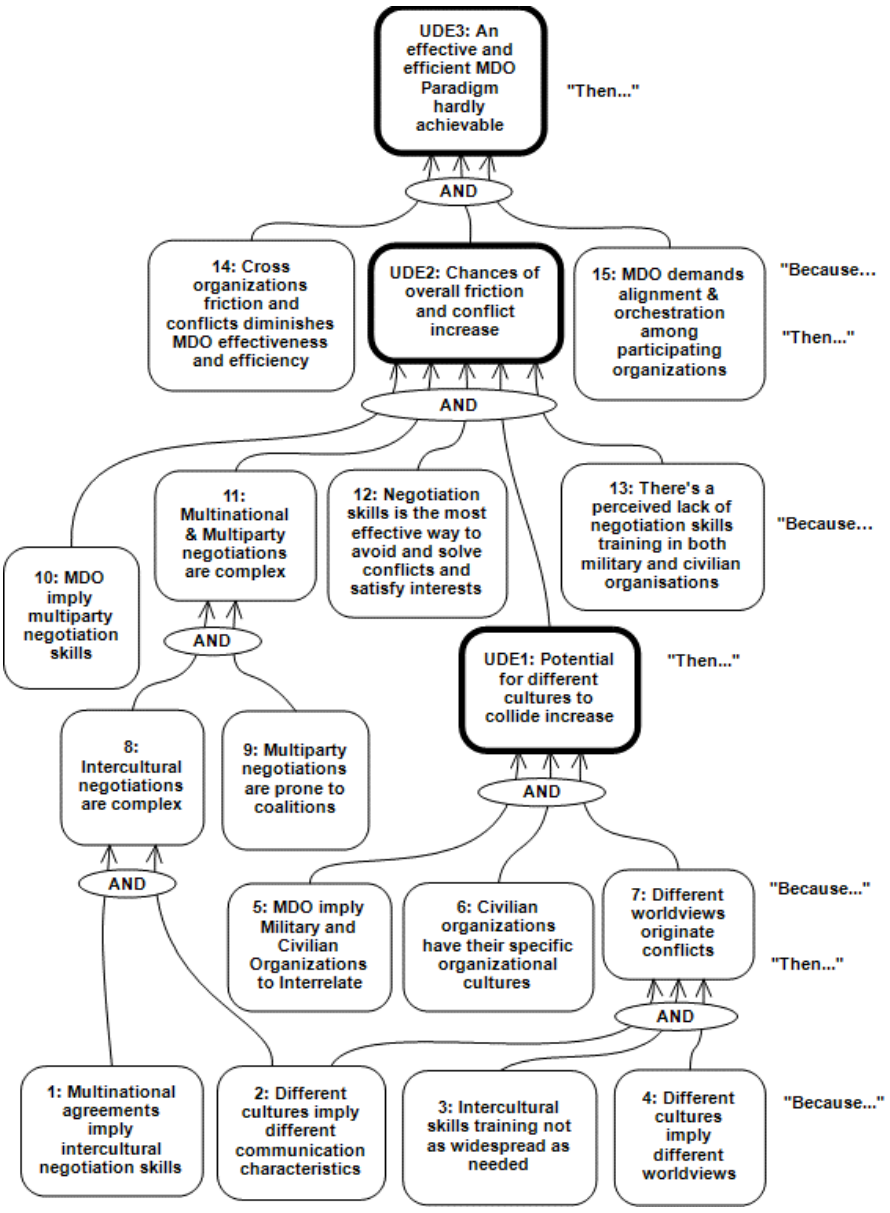
The results from the methodological approach are shown as logic trees. The *Current Reality Tree* captures the analysis and diagnosis of the current paradigm. Another logical tree represents the solution, the *Future Reality Tree* [FRT]. Such trees were designed by logical validation by following the Categories of Legitimate Reservation (Dettmer, 2003).

Current Reality Tree, or defining the problem

The Current Reality Tree [CRT] is a TOC logic tree that helps in the analysis and diagnosis of the problem at hand. It identifies the Undesirable Effects [UDE] and shows the chains linking them down to the originating root causes (Figure 2).

The CRT is a TOC logic tree that should be read from the bottom up as "if A and B … then C," which is self-explanatory. In this case, the root causes identified in boxes 1-6 and 9 are the roots of the visible undesirable symptoms, specifically UDE1 – 3, of which UDE3 represents the negation of the overall Goal—an *effective and efficient MDO Paradigm hardly achievable*.

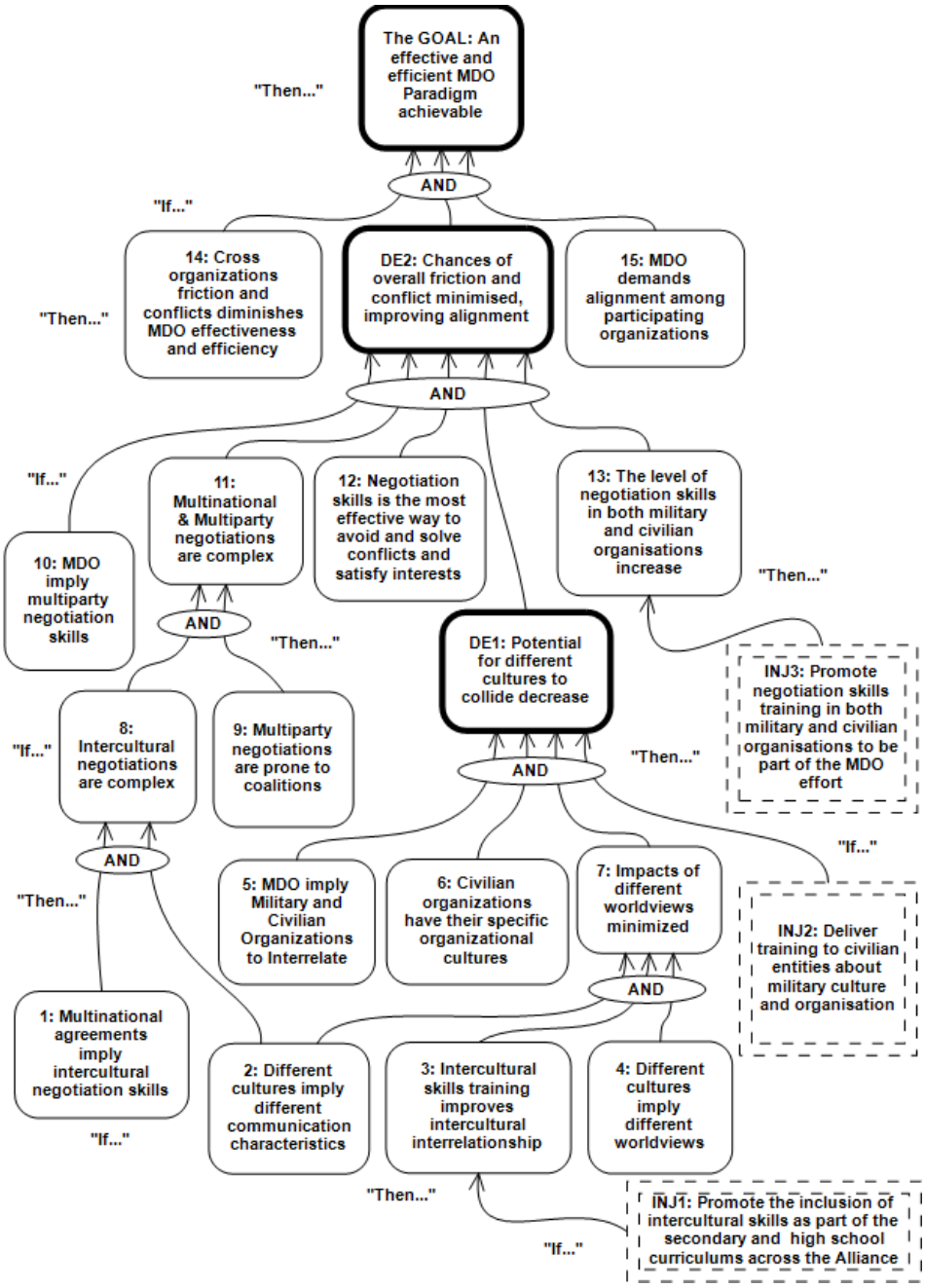
Figure 9. 2: *CRT - defining the problem links the UDEs to root causes*



Future Reality Tree, or designing the solution

Once the CRT characterised the problem, one can design workable solutions by injecting measures inspired by organisational principles presented in the background section. The TOC suggests three ways to generate actions to be injected into the CRT, which will reverse or mitigate the UDEs (*UnDesirable Effects*): Use of Evaporating Clouds, a TOC tool; injecting an action that eliminates or minimises UDEs, and creating an injection which satisfies a critical success factor (Dettmer, 2003). Such actions, INJ1-3, are visible in the FRT (Figure 3).

Figure 9. 3: *FRT – designing the solution through injections INJ 1-5*



As depicted in the FRT, three injections (INJ1-3) are now considered, reversing the previous UDEs and allowing the goal to be attained at the top. These injections can be understood by reading them as: "INJ1: … *by promoting the inclusion of intercultural skills as part of the secondary and high school curriculums across the Alliance* " intercultural relationships will be improved (future), which after a chain of cause-and-effects will give rise to DE1 (*Potential for different cultures to collide decreases*). Then, the contributions of DE1 (*Potential for different cultures to collide decreases*) and INJ3 (*Promote negotiation skills training in both military and civilian organisations to be part of the MDO effort*) contribute to achieving the desired effect of DE2

(*Chances of overall friction and conflict minimised, improving alignment*). Following the same rationale, DE2 (*Chances of overall friction and conflict minimised, improving alignment*) will be a net contributor to achieving the goal – DE3 (*An effective and efficient MDO Paradigm achievable*).

Another issue identified during the problem characterisation stage (also known as the current reality tree-building state) is that civil actors, who are an enabling factor for MDO, typically struggle to understand military culture, military operations, and the overall military *modus operandi*. Therefore, some action shall be taken to close the gap between such distinct realities, and that is precisely the function of injection INJ2 (*Deliver training to civilian entities about military culture and organisation*). Moreover, boxes 14 and 15 are represent issues that while they cannot typically be totally eliminated, they can however be considered as context or environmental factors to count on while designing the FRT.

When building Future Reality Trees, such as the one illustrated in Figure 3, it is essential to check for the potential existence of "negative branches." Negative branches are feedback mechanisms that typically originate collateral or unintended effects. If such negative branches develop, adequate solutions shall be designed to mitigate or eliminate them, specifically through prerequisite trees, as presented in the discussion section.

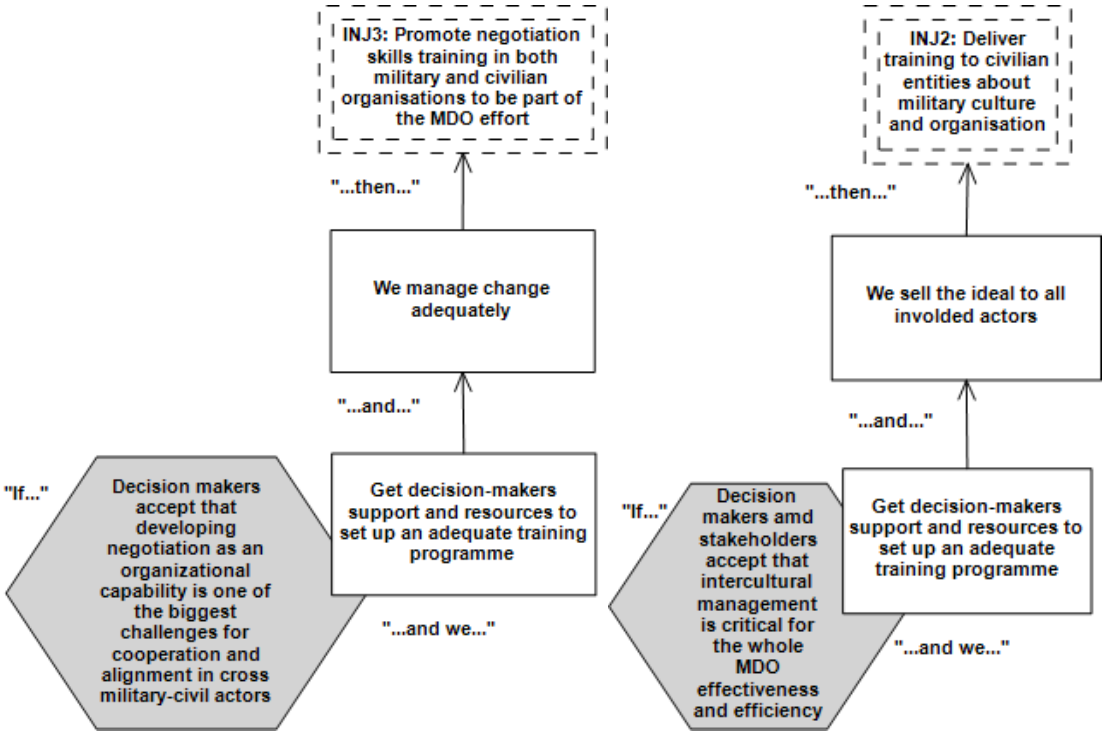
Discussion

The designed solution illustrates the TOC process – a framework for solving complex problems progressively. Some practitioners disregard academics for their too theoretical or abstract approaches to problems. The framework used in this text helps fill such a gap by providing a pragmatic, deployable framework that facilitates the design of solutions, strategies, or even policies to support the right endeavour for achieving organisational and inter-organisational goals. The rationale for the developed model, with its cause-and-effect relationship, is based on Aristotelian logic. By identifying what to change and what to keep, we end up with actions to be injected into logic chains, which drive our organisational systems towards the desirable objectives. However, such actions may not be enough to ensure sufficiency in achieving the desired paradigm. To ensure a successful implementation, it needs to address the question of '*how to cause the change*?'.

Some authors signalled the importance of not underestimating the resistance to change as a constraint on itself (Kotter, 1996; Sull et al., 2015). To achieve the desired goals, the TOC framework utilises prerequisite trees, a type of tree or branch that ensures implementation will develop more smoothly. Prerequisite trees are built to ensure the "strategic injections" are implemented in practice and obstacles are removed or mitigated to acceptable levels. Figure 4

illustrates the prerequisite tree regarding injections INJ2 and IN3 within the context of the developed model.

Figure 9.4: *The prerequisites tree for injections INJ2 and INJ3*



Training is highlighted as part of the proposed solution. However, this should be understood broadly, beyond the mere acquisition of knowledge and skills; training also promotes networking and relationship building – something essential if one is honest about achieving an effective and efficient MDO paradigm. Moreover, the designed solution for such a strategic problem would benefit from checking all measures against the known DOTMLPFI checklist of organisational variables (Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities, and Interoperability) in order to clarify any additional constraints further as needed regarding implementation (Lofgren, 2016).

Conclusion

This chapter and the underlying research employ logical validation based on the Categories of Legitimate Reservation (Dettmer, 2003). The solution [FRT] serves as a starting point for more comprehensive research aimed at specific contexts, industries, or businesses to achieve an MDO paradigm, where military and civil organisations collaborate for an overall ‘emergence’ of desirable effects. Once the analysis and diagnosis are complete using a clarifying CRT, and a solution is designed employing an FRT, implementation follows to deploy the solution while maximising the

chances of harnessing complex operations. Any deployment, however, needs some form of enabling conditions for its success.

In short, MDO can be understood as a function of SoS as it will depend on an underlying SoS infrastructure made of technological and organisational systems: $MDO = f(SoS)$. A SoS, especially the collaborative and acknowledged types, depends on agreement mechanisms among the constituent organisational systems: $SoS = g(Negotiation)$. Therefore, one could envision a composed function where, in the end, *negotiation as an organisational capability* is a key enabler for MDO success, $MDO = f(g[Negotiation])$, and where SoS and Negotiation skills are key domains to develop and harness across the relevant participating organisations. Considering negotiation as a key organisational capability, it should be included at the core of education and not as a rare subject. For instance, it is challenging to find military academies, schools, and military education organisations offering such courses, with the US West Point Negotiation Project [WPNP] and the US Air University Negotiation Centre [USAFNC] being notable examples. Some Staff colleges may offer it as a subject alongside a range of core subjects, but not to the same level of prominence it deserves. Such a critical subject for achieving MDO should be brought to the core of education and training, with meticulous attention to quality, aligning with the best in class worldwide, among others, the Program on Negotiation (HLS, 2024) and Negotiation Strategies (HKS, 2024).

This study represents a first cut into the critical role negotiation, as an organisational capability, will have to play in gathering distinct organisations to contribute to achieving the MDO paradigm. Therefore, further research is needed to deepen our understanding of the topic. Regardless of the broader MDO concept, this text has a focus on the Military – Civilian integration, which may end up being one of the weakest links in the chain towards achieving a truly MDO paradigm, as such attainment may have many potential spheres of friction due to different organisational cultures, different country cultures, and different levels of interests among military and non-military organisations which shall cooperate to achieve an effective MDO paradigm.

Acknowledgement

The authors would like to acknowledge the Portuguese Navy Research Centre (CINAV) for its support.

References

ACT. (2023). *MDO Conference*. NATO ACT, Copenhagen, Denmark. 9-11 Oct.

Axelrod, R. (1984). *The Evolution of Cooperation*. New York: Basic Books, Inc., Publishers.

Burns, J.R. & Musa, P. (2001). “Structural Validation of Causal Loop Diagrams”, in Hines, J.H., Diker, V.G., Langer, R.S. and Rowe, J.I. (Eds.), *Proceedings of the 19th International Conference of the System Dynamics Society*, presented at THE 19TH INTERNATIONAL

CONFERENCE OF THE SYSTEM DYNAMICS SOCIETY, System Dynamics Society, Atlanta, GA.
Dahmann, J.S. (2015). *Systems of Systems Characterization and Types*. STO EDUCATIONAL NOTES. STO-EN-SCI-276. 30-31 Jan.
Dailey, A. M. (2023). Multi-Domain Operations & Synchronization with Non-Military Instruments of Power. *NATO Multi-Domain Operations Conference 2023*. Copenhagen, 10-11 October.
Dettmer, H.W. (2003). *Strategic Navigation. A Systems Approach to Business Strategy*. Milwaukee, Wisconsin: ASQ Quality Press.
Dettmer, H. W. (2007). *The Logical Thinking Process. A Systems Approach to Complex Problem Solving*. Milwaukee, Wisconsin: ASQ Quality Press.
HKS, (2024). Negotiation Strategies: Building Agreement Across Boundaries program at Harvard Kennedy School https://www.hks.harvard.edu/educational-programs/executive-education/negotiation-strategies#online-vs-on-campus-schedule, [Assessed on 3rd Aug. 2024]
INCOSE (2018). *Systems of Systems Primer*, INCOSE-TP-2018-003-01.0.
Emmeche, C., Koppe, S., and Stjernfelt., F. (1997). "*Explaining emergence*: Towards an ontology of levels." *Journal for General Philosophy of Science,* vol. 28, no. 1, pp. 83-119.
Goldratt, E.M. (1990). *Theory of Constraints*. Great Barrington, Massachusetts: North River Press.
Goldratt, E.M. (1992). *The Goal*. Great Barrington, Massachusetts: North River Press.
Lewicki, R. L., Barry, B., & Saunders, D. M. (2007). *Negotiation*. New York, McGraw-Hill.
Lofgren, (2016). NATO Capability Development Interoperability. The Three Swords Magazine. Last accessed on June 23 2010 (http://www.jwc.nato.int/images/stories/_news_items_/2016/LT_GEN_Lofgren_interview.pdf)
Kotter, J. P. (1996). *Leading Change*. Harvard Business School Press. Boston, MA: USA.
Rihani, S. (2002). *Complex Systems Theory and Development Practice. Understanding Non-Linear Realities*. London, UK: ZED Books.
Scheinkopf, L. J. (1999). *Thinking for a Change. Putting the TOC Thinking Processes to Work*. Milwaukee, Wisconsin: ASQ Quality Press.
Schragenheim, E. (1998*). Management Dilemmas. The Theory of Constraints Approach to Problem Identification and Solutions*. New York: CRC Press.
Snowden, D., Boone, M. E. (2007). A Leader's Framework for Decision Making. *Harvard Business Review*. November.
Snowden, D., Rancati, A. (2022). *Managing complexity and chaos in times of crisis. A guide for decision-makers inspired by the Cynefin framework*. Luxembourg: Publications Office of the European Union.
Sull, D., Homkes, R., Sull, C. (2015). Why Strategy Execution Unravels—and What to Do About It. *Harvard Business Review*. March.
USAFNC, United States Air Force Negotiation Centre, https://www.airuniversity.af.edu/AFNC/ [Assessed on 3rd Aug. 2024]
Weick, K.E., Sutcliffe, K.M. (2015). Managing the Unexpected. Sustained Performance in a Complex World (3rd Ed.). Hoboken, New Jersey: Wiley.
WPNP, West Point Negotiation Project, https://www.westpoint.edu/research/centers-and-institutes/west-point-leadership-center/west-point-negotiation-project [Assessed on 3rd Aug. 2024]

Chapter 10: A Contemporary Taxonomy of Information Warfare: An Analysis Proposal Based on Scientific Production

Mariana Grilli **Belinotte**, ORCID: https://orcid.org./0000-0003-0031-597X
Luiz Rogério Franco **Goldoni**, ORCID: https://orcid.org./0000-0001-5257-9470

Abstract:
This paper proposes a contemporary taxonomy of information warfare based on bibliometric and thematic content analyses of scholarly literature. The study examines 1,909 publications (804 peer-reviewed articles) from 1982-2024, identifying five distinct periods in the field's evolution: Early Years (1982-1996), Establishment (1997-2005), Consolidation (2006-2015), Digital Expansion (2016-2019), and Contemporary Era (2020-2024). Through qualitative analysis of 32 highly-cited articles, the research classified scholarly conceptualisations according to three primary dimensions: target (information vs systems), destinatary (society vs military), and technological dependency. Findings reveal that 65.6% of analysed articles identify information as the primary target and society as the main destinatary, with varying perspectives on technology's role. Over time, the field has shifted from broader conceptualisations encompassing cyberattacks and technical interference towards narrative disputes, symbolic manipulation, and informational control. The analysis also indicates increasing theoretical sophistication and methodological rigour in recent literature, with growing attention to propaganda, values, public opinion, media, and information control. Contemporary Russia features prominently in current discourse, reflecting its perceived centrality in information warfare practices. This taxonomy contributes to a more nuanced understanding of how academic literature has approached information warfare, highlighting conceptual evolutions without prescribing definitive boundaries. The study acknowledges limitations regarding Global North dominance in academic publishing and suggests that future research explore citation dynamics and the field's impact on policy formation.

Key-words: information warfare; bibliometric analysis; security studies, information operations; thematic content analysis.

Introduction

The significance of information in conflict is longstanding — its use for political, strategic, and tactical purposes has been documented for millennia (Sun Tzu 2010; Thucydides 2009; Fuller 2002; Keegan 1996; Liddell Hart 2010). Technologies such as computers, mobile phones, and social media have introduced new forms of interaction and communication, which in turn have

transformed how information is acquired, processed, used, and disseminated (High et al. 2023; Zhang & Lin 2023).

The twenty-first century has witnessed an intensification of disputes and conflicts increasingly shaped by information (Castells 1999; Nye 2011). In this context, it is essential to understand how the terms ***information war*** and ***information warfare*** have been used in academic discourse.

Understanding the use of a term within academia is not a mere theoretical, epistemological, or ontological exercise. In the fields of security and defence—where the boundaries between academic, political, and practitioner domains are particularly blurred—the terminology employed can influence the formulation and implementation of military doctrines or security and defence strategies and policies (Baldwin 1997; Williams 2007; Stritzel 2014). Overly narrow academic interpretations may lead to incomplete or ineffective policies, while excessively broad ones risk generating unworkable or unrealistic approaches.

We approach concepts as being shaped by context—implying that their meaning varies across time, space, and usage (Skinner 1969; Taylor 1985; Hall 1997; Foucault 2002; Wittgenstein 2009). Information war/warfare is no exception. Academic texts on the subject differ significantly: some downplay the role of technology, while others place it at the center; some include military actors as key targets of campaigns or attacks, while others exclude them; certain works identify the system as the primary target, while others focus on information itself.

For the purposes of this analysis, we adopt a broad operational definition of information warfare as the deliberate use of information, communication, and related technologies to influence, disrupt, or control perceptions, behaviors, and systems in pursuit of strategic objectives. These conceptual variations are also closely linked to the broader evolution of hybrid threats, which combine conventional and unconventional means above or below the threshold of armed conflict (Marsili 2021).

In light of these divergent approaches and interpretations, two guiding questions arise: “in what sense(s) are scholars using the terms information war/warfare?” and “what are these terms being used to describe or propose?”. These questions offer a more meaningful and analytically useful approach than the pursuit of a single, definitive answer to “what is information war?”

The primary aim of this research is to develop a contemporary taxonomy of the actions and strategies associated with the concept of informational warfare. The specific objectives are: (a) to analyse the range of actions categorized as “information warfare”; (b) to classify and organise these actions according to the predominant medium, instrument, and objective; and (c) to map the relationships between these strategic categories through visual representation.

This study also addresses a gap in the literature by assessing the broader academic output on the topic, identifying prevailing themes and dominant perspectives. This may help uncover underexplored areas and provide a clearer understanding of the current scholarly landscape.

One clear limitation of the study is the impossibility of reviewing the entire body of academic literature on the subject. Nonetheless, we acknowledge that academia itself "selects" what it deems relevant, a process often reflected in citation patterns (Bourdieu, 1989; Latour & Woolgar, 1997; Bornmann & Daniel, 2008). Additionally, the dataset is skewed toward anglophone production, which may reinforce an English-language and Global North bias in the taxonomy presented here, limiting the visibility of alternative conceptualisations and regional experiences. Future research could address this by incorporating non-English sources and expanding the scope to include underrepresented regions and perspectives.

Accordingly, the first step was to identify the most frequently cited texts in the field and then examine how they frame and engage with the subject. To this end, we adopted a methodological approach grounded in bibliometric analysis and thematic content analysis. In response to the specific challenges posed by developing a contemporary taxonomy of the field, we devised a tailored methodology that integrates these two techniques.

The methodology is outlined in the next section, followed by a presentation and visual analysis of the data. This includes a review of the evolution of academic research on the topic and an assessment of how scholars have conceptualized and applied the idea of information warfare. Beyond informing our taxonomy, this detailed methodological exposition also aims to serve as a practical example for researchers interested in applying similar approaches in the field. Readers who wish to focus solely on the conceptual outcomes may skip this section without losing the main arguments.

Methodology

The research employed two methods: bibliometric analysis and thematic content analysis. Bibliometric analysis enables the examination of the evolution and structure of a specific field, area or theme. This method makes it possible to assess trends in the increase or decrease of production and distribution of citations (Yu et al., 2021). Thematic content analysis, on the other hand, allows for the identification of thematic patterns within a set of articles, reports, interviews, news or other types of documents, whilst also supporting the development of categorizations (Saldaña, 2013).

Bibliometric analysis was adopted not only to describe the development of the field of study in question, but also to inform the selection of articles used in the thematic content analysis. By providing an overview, the bibliometric analysis grounded the selection of the most relevant

articles, taking into account the number of citations and publication patterns. The following sections will present the procedures adopted for each of these methods, as well as the results obtained through their application.

Bibliometric analysis

The bibliometric analysis procedure adopted here is inspired by the PRISMA protocol, developed by researchers in Biological and Health Sciences, aimed at standardizing systematic reviews (Abusaada & Elshater 2022; Dekker et al., 2019; Liberati et al. 2009). The version used in this research was adapted for Social Sciences and comprises the steps shown in Table 1:

Table 10.1: *PRISMA protocol steps*

Preparation	Definition of initial keywords based on the literature in the field
	Definition of search strings
	Selection of the database
Data Collection	Search for the search strings in the Scopus database, within the Title, Abstract, and Keywords fields
	Download of metadata in .csv formats
Data Cleaning and Normalisation	Data verification using Numbers, R and R Studio
	Exclusion of categories with insufficient data
Data Analysis	Description of the material
Visual Representation	Use of R, RStudio and packages such as ggplot2 and dplr
Discussion	Interpretation of the results in relation to existing literature and identification of potential research gaps

Source: adapted by the authors for the social sciences from Liberati (2009).

Data collection was conducted on 10 March 2025,[1] using the Scopus indexer (scopus.com). The Scopus indexer was chosen for being a comprehensive and qualified database, even when compared to others such as Google Scholar and Web of Science, and for having tools that facilitate the collection and processing of these data, such as downloading large volumes of data in .csv format (Harzing & Alakangas 2016; Singh et al. 2021).

[1] This period represents the span from the first result found in the database to the end of 2024, which was established as our cutoff date for data collection.

The search string used was '"information* war" OR "information* wars" OR "information* warfare"', and the fields searched were Title, Abstract and Key-words. The data were stored in csv format, both physically and digitally, under the responsibility of the researchers. As these were publicly accessible and non-sensitive data, a data treatment plan was not elaborated; priority was given only to their conservation and integrity.

The R programming language was used to process and analyse the data. The RStudio environment and various specialized packages were employed, such as tidyverse, which includes tools like dplyr and tidyr, and ggplot2, which allow a high degree of control in creating visual representations. Additionally, artificial intelligence assistants were incorporated to optimize code development.

The search found a total of 1,909 results, covering the period from 1 January 1965 to 31 December 2024. Among these documents, 804 were identified as scientific articles published in peer-reviewed journals. The results are presented in Section 3.

Articles selection

This section describes the criteria for selecting the articles analysed and the methodological procedures adopted in the primary and secondary analyses. The selection of works to be included was one of the central challenges of the research, as it required establishing parameters to assess the relative importance of each period and each article—using citation count as a proxy for relevance, but with important caveats.

The main obstacle was the significant disparity in publication volume across periods (from 8 articles,[2] in the earliest period, to 270 in the final period), combined with extreme variations in citation patterns (from 0 to 250 citations per work). Adopting a fixed number of articles to be analysed per period, or homogeneous time intervals, could lead to distortions, such as the loss of relevant articles. Simultaneously, using citation count as the sole criterion could distort the analysis of temporal evolution. Therefore, mixed criteria were adopted to achieve a more sophisticated methodological solution.

Initially, the periods were defined based on three main axes, according to specialized literature in geopolitics, International Relations and technology studies. The first one is historical and technological milestones (such as the advent of social networks and significant geopolitical events); the second one is the theoretical trajectory of the field, identified in previous literature reviews; and the third one are publication patterns revealed by preliminary bibliometric analysis.

[2] Only one article, from Period 1 (Early Years, 1982-1996), was excluded from the qualitative analysis as its subject matter was unrelated to information warfare despite matching the search criteria.

This triangulation allowed for the establishment of five distinct phases: Early Years (1982-1996), characterised by the first conceptual efforts; Establishment (1997-2005), marked by the institutionalization of the field; Consolidation (2006-2015), of theoretical maturation; Digital Expansion (2016-2019), with the incorporation of digital platform dynamics; and Contemporary Era (2020-2024), of the most recent developments. This division was then validated through a changepoint analysis,[3] which identified statistically significant transitions in publication volume, corroborating the proposed temporal divisions. The five proposed periods have their own characteristics in terms of publication volume and historical-technological context:

- *Early Beginnings (1982-1996):* embryonic phase, with few publications, but which established the first meanings and theoretical frameworks on the concept of "information warfare", in a pre-Internet context. The fall of the Berlin Wall (1989) and the collapse of the USSR (1991) also strongly influenced this period, especially in International Relations, Security Studies and Military Sciences.
- *Establishment (1997-2005):* field consolidation phase, coinciding with the expansion of the commercial internet and the 9/11 attacks. These events drew the attention of the public and the political class to the then-emerging cyber threats. The new geopolitical challenges, such as terrorism and hacker attacks, in a world that had experienced a period of relative calm after the Cold War, reignited debates focused on international security and defence. Production and citation numbers increased significantly.
- *Consolidation (2006-2015):* period marked by notable cyberattacks—such as those perpetrated against Estonia in 2007 and the Stuxnet case—by the popularization of social networks, whose mobilizing power was evidenced, for example, in the Arab Spring (2010- 2012), and by the operationalization of cyberspace for espionage activities, as revealed by Edward Snowden in 2013. The continuity of the terrorist threat and the emergence of new non-state actors in cyberspace also impacted research agendas. The number of publishedarticles is similar to the previous period, but the total citations increased.

[3] The changepoint analysis was conducted using the R changepoint package, which automatically identifies the years in which significant changes in publication patterns occurred. The method works by dividing the time series into distinct segments, with each segment representing a period with homogeneous statistical characteristics in terms of academic production. The algorithm examines the series year by year, detecting moments when: the average number of publications undergoes a significant change, the variability of the data changes substantially, and these changes cannot be explained by random variations. The approach used (PELT - Pruned Exact Linear Time) is particularly efficient for humanities datasets, as it considers the discrete nature of count data (number of articles), automatically adjusts to the size of the time series, and provides robust results even with annual fluctuations. This method complements, but does not replace, the qualitative analysis of the identified historical contexts. For a more detailed explanation, see: Killick, R., & Eckley, I. (2014). changepoint: An R Package for Changepoint Analysis. Journal of Statistical Software, 58(3), 1-19.

- *Digital Expansion (2016-2019):* paradigmatic events such as the US presidential elections (2016), the Brexit referendum (2016) and the Cambridge Analytica scandal (2018) highlighted the strategic and political importance of social networks and cyberspace as a whole. In just three years, almost twice the number of articles from previous periods were published, and total citation count was close to, but higher than, the third period.
- *Contemporary Era (2020-2024):* Current phase defined by the global COVID-19 pandemic and the Russo-Ukrainian war (since 2022), which showed both the importance of cyberspace for services, transactions and daily activities, as well as for traditional conflicts and global geopolitics as a whole. Again, the number of published articles doubled compared to the previous period, but the number of citations remains similar, likely due to the short time elapsed between publications and analysis.

Below, the periodisations based on qualitative analysis and statistical changepoint detection are presented in Figures 1 and 2. Table 2 compares these results, showing the time intervals of each periodisation format, revealing significant convergence between the qualitative and statistical approaches. This agreement between distinct methods strengthens the reliability of the proposed periodisation, supporting the use of the identified periods for the subsequent selection of articles for further qualitative analysis.

Figure 10.1: *Article dispersion by year and number of citations, distributed in qualitatively determined periods.*

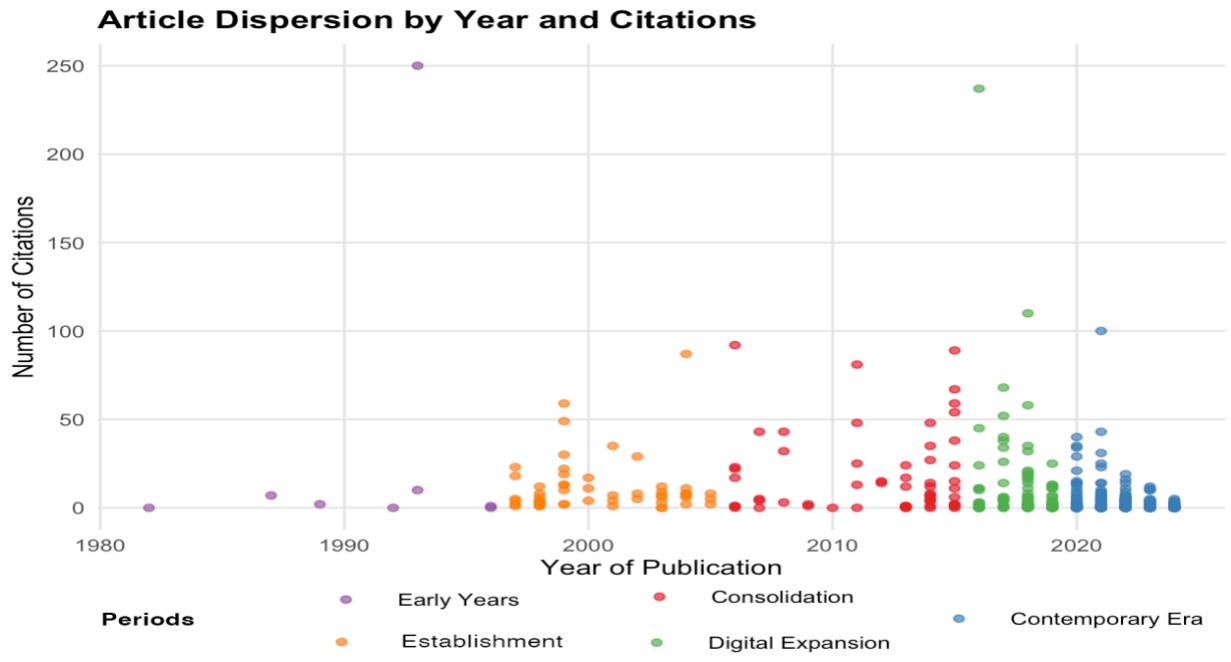


Figure 10 2: *Publication patterns as analysed using changepoint package.*

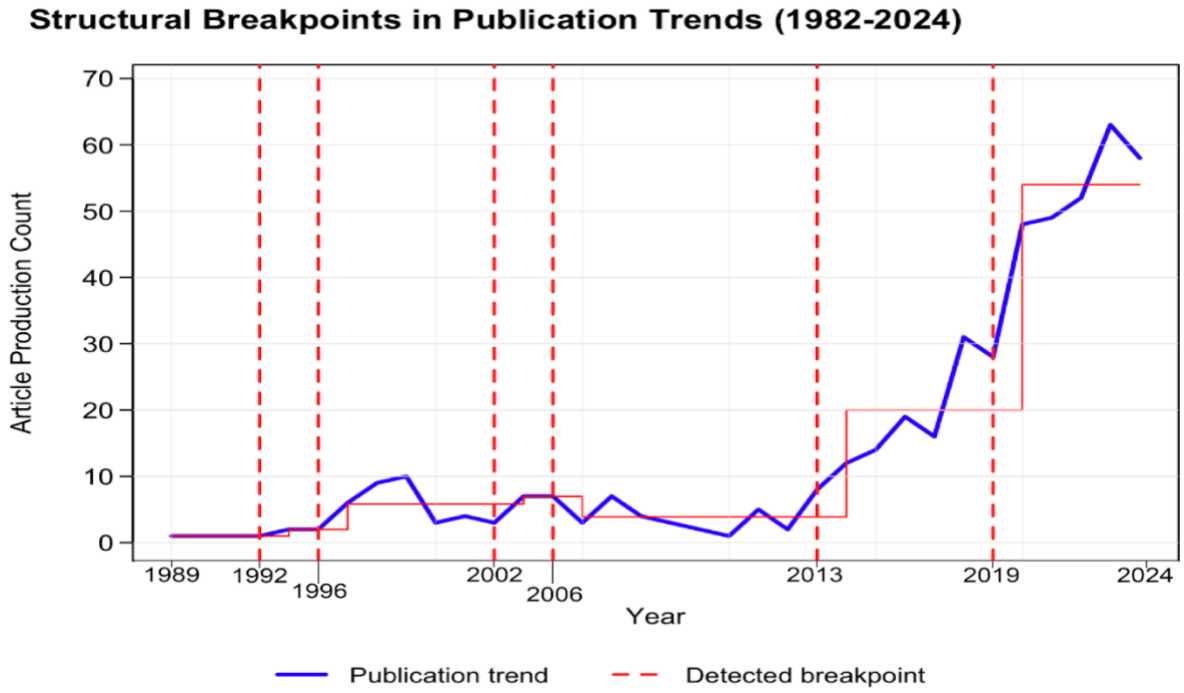


Table 10. 2: *Comparison of periodisations obtained through qualitative analysis and statistical changepoint detection.*

	Qualitative proposal	Changepoint proposal
Period 1	1982-1996	1982-1992; 1993-1996
Period 2	1997-2005	1997-2002; 2003-2006
Period 3	2006-2015	2007-2013
Period 4	2016-2019	2014-2019
Period 5	2020-2024	2019-2024

It is important to acknowledge that this periodisation—along with the data collection process and the broader scientific output—is predominantly reflective of developments in the Global North, and more specifically, of events as they unfold in the United States. This represents both a limitation of the present study and a manifestation of enduring asymmetries in global knowledge production. The hegemony of English as the dominant academic language not only

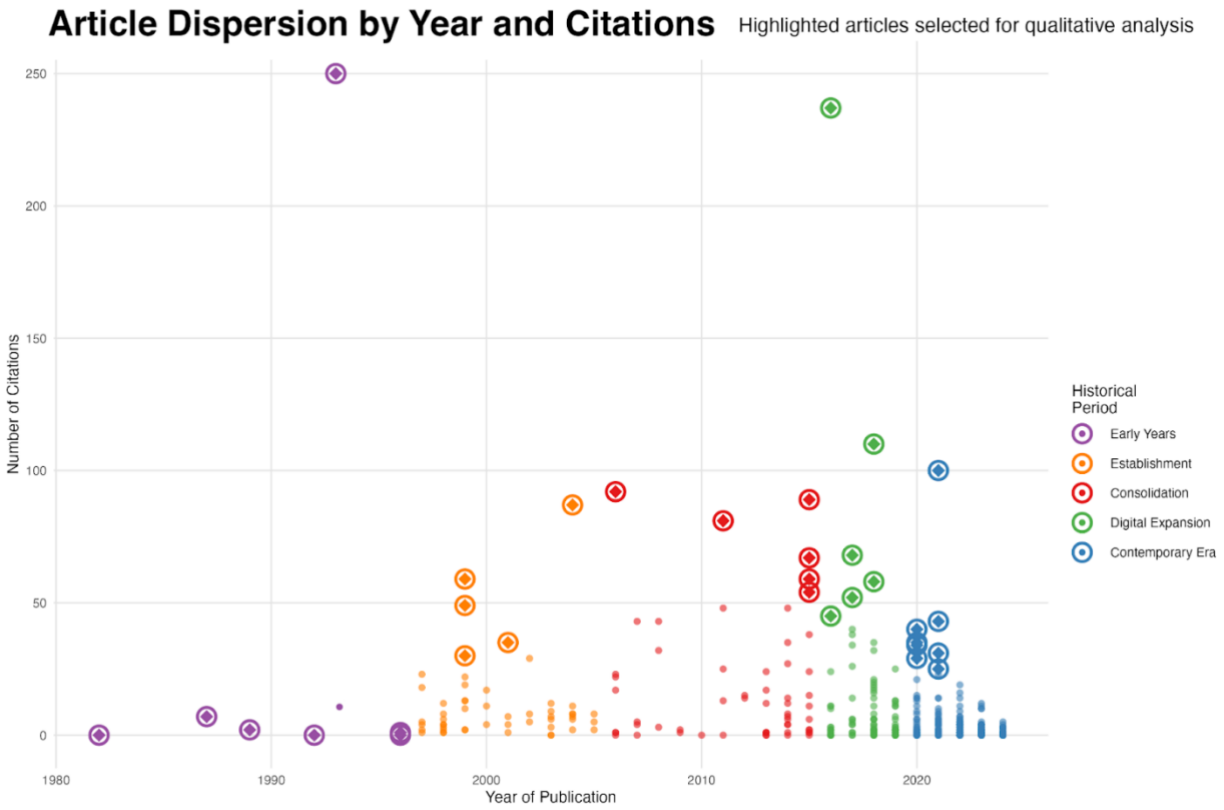
shapes which research gains international visibility and recognition, but also influences which phenomena are deemed legitimate subjects of scientific inquiry. Consequently, the experiences, contexts, and theoretical contributions of countries in the Global South are frequently marginalized or rendered invisible within major scientific repositories, perpetuating a cycle in which the sociotechnical realities of certain regions are treated as universal, while others are framed as particular or exceptional (Santos, 2017). This bias is not merely methodological but structural, reproducing within academia the same inequalities that characterize global economic, political, and cultural relations.

To illustrate: according to the SCImago Journal & Country Rank, within the field of Political Science and International Relations, there are currently 658 indexed journals. Of these, 409 are published in Western Europe (including 255 in the United Kingdom) and 109 in Northern America (105 in the United States). This means that 78.7% of the indexed journals in the field are based in the so-called Global North, with 54.7% published exclusively in the UK and US. Among the 162 journals ranked in the first quartile (i.e. those with the highest impact), only 7 (4.3%) are published outside the Global North (Scimago, 2025).

Thematic Content Analysis

Once the periods had been defined, a set of articles was selected for qualitative analysis. The final selection aimed to balance both the time of publication and citation count, using a compensatory approach: in the Early Years phase, all seven articles were included due to their seminal importance, even if they have received few citations. In the Establishment and Consolidation periods, articles with at least 30 and 54 citations respectively, were prioritised, capturing the most influential contributions. For the Digital Expansion and Contemporary Era, the thresholds were adjusted to 45 and 25 citations, respectively, taking into account the shorter citation window for more recent publications. This approach led to the selection of 32 articles that reflect both foundational work and current debates, enabling the identification of conceptual continuities and shifts over time. The full list of selected articles is available in Appendix 1.

Figure 10.3: *Article dispersion by publication year and citations. Highlighted articles were selected for qualitative analysis.*



The 32 selected articles were examined through thematic content analysis. This is a qualitative method designed to identify, analyse, and report patterns of meaning (themes) within a data set, such as interview transcripts, reports, videos, images, or survey responses (Braun et al. 2024; Saldaña, 2013). It enables the systematic organization and interpretation of data by assigning codes—short words or phrases that capture the core meaning of relevant excerpts—for the subsequent development of themes (Saldaña, 2013).

Thematic analysis is known for its flexibility: although it follows a structured process, it allows researchers to adapt the steps based on their aims and the specific context of the study (Vaismoradi et al., 2013). Its main purpose is to provide a clear and organized understanding of emerging patterns in the data, without requiring a high degree of interpretation, which makes it especially suitable for studies aiming to describe and summarise findings in a straightforward way (Vaismoradi et al., 2013). It is also important to acknowledge the subjective nature of this approach, as coding and theme identification are shaped by the researcher's perspective and experience, which may lead to different interpretations across analysts (Saldaña, 2013).

This study employed both primary and secondary analyses. The primary analysis aimed to classify the articles according to the target of information warfare, the intended audience of such actions, and the degree of technological dependence mentioned by the author(s). First, categories

and their respective classifications were developed based on prior readings of the relevant literature. Then, using the full article as the unit of analysis, each article was assigned a classification within each category. The categories and their classifications are presented below.

In the target category, three classifications were defined: 0, 1, and 2. Classification 0 refers to articles in which the authors consider information itself as the main target of warfare—that is, the manipulation of perceptions and narratives, the creation of content for dissemination, or the alteration of electronic data, without damage to or modification of the systems involved. Classification 1 includes articles that mention attacks or alterations affecting both information and systems. Examples include the manipulation of algorithms to amplify message reach or hacking into systems to insert false information. Classification 2 refers to attacks directed primarily at systems. These may still involve data alteration or damage, but the main objective is to affect the systems that store or transmit the information.

The destinatary category also comprises three classifications. Classification 0 includes articles that refer to the general public or specific societal groups as the target audience. Classification 1 applies to articles that address both civilian and military audiences. Classification 2 relates to articles focused on military recipients, whether referring to combatants or systems used by the armed forces and related institutions.

Finally, the technological dependence category comprises four levels. Classification 0 includes articles in which the use or reliance on technology is minimal: systems are either not mentioned or referenced only superficially. Classification 1 refers to articles where technology is mentioned as a support or complementary tool. Classification 2 includes articles about which technology is considered essential to the actions described. Lastly, classification 3 covers articles in which the discussion on technology use overrides other aspects, for instance, articles offering detailed accounts of social media manipulation strategies. Table 3 summarizes and facilitates the visualization of the coding applied in this chapter.

Table 10.3: *Coding scheme used to classify the articles by target, destinatary, and tech dependency.*

Classification	**target**	**destinatary**	**tech**
0	Information	Society	Minimal/no mention
1	Information and systems	Society and military targets	Support
2	Systems	Military targets	Indispensable
3			Overrides other aspects

Articles discussing theoretical aspects—such as press regulation, the nature of social relations, broad societal changes, and narrative construction—were generally classified as target_0, destinatary_0, and tech_0.

The secondary analysis was contextual and conducted in an exploratory manner; that is, the categories were created as they emerged from the articles, and the unit of analysis ranged from a single sentence to multiple paragraphs. It is important to highlight that thematic content analysis, used in both the primary and secondary analyses, is a descriptive tool. It aims to identify the presence of themes within a set of documents. In this sense, the analysis does not assess whether a particular author agrees or disagrees with a given theme, but simply whether the theme is addressed in their article.

The software MaxQDA was used due to its ability to systematically organise, code, and retrieve qualitative data, enhancing both the management of the analysed material and the subsequent interpretation. The program allows researchers to classify text excerpts under thematic codes, making it easier to identify patterns and export data for further analysis. Additionally, its advanced search and recurrence visualization tools speed up the identification of relevant examples, while its annotation and data-linking features support the development of more robust interpretations. As such, MaxQDA not only structures the analytical process but also broadens the possibilities for exploring the data, both through qualitative approaches and, where applicable, through integration with quantitative analysis.

After reading the articles and defining the applicable codes for each, the codes created during the secondary analysis were refined by removing categories that were rarely used or not sufficiently representative. For instance, subcategories within the “theory” category—such as post-structuralism, constructivism, realism, and liberalism—were merged into the higher-level category “theory”. Similarly, subcategories such as “invasion of Panama” and “UN Security Council” were discarded for encompassing too few articles. With the methodological procedures being detailed, the following section presents the main findings of the study and explores the patterns identified.

Results

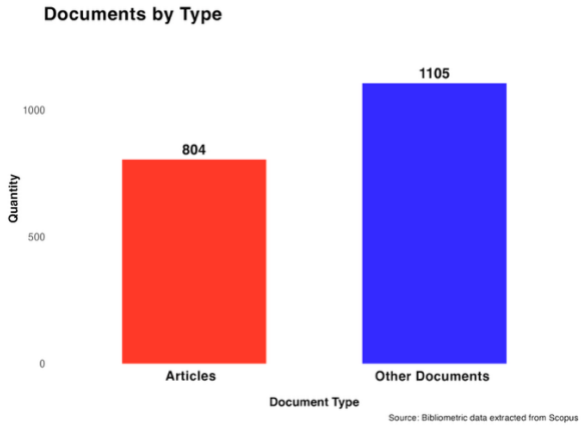
This section analyses the results of the bibliometric and thematic content analysis. In several figures, data from the earliest years have been omitted due to the limited number of publications during this period, which would otherwise overly compress the visual representation and diminish clarity.

A total of 1,909 results were identified, including 804 scholarly articles and 1,105 other types of publications. Among the articles, 625 were published in English, 10 in Ukrainian, 77 in

Russian, 71 in Chinese, 5 in German, 3 in Arabic, 2 in Italian and Lithuanian, and one each in French, Polish, Portuguese, and Romanian. Among those selected for qualitative analysis—using citation count as a proxy for relative importance—all were published in English. This indicates a clear dominance of English within the field, both in terms of publication and in the selection of articles for citation.

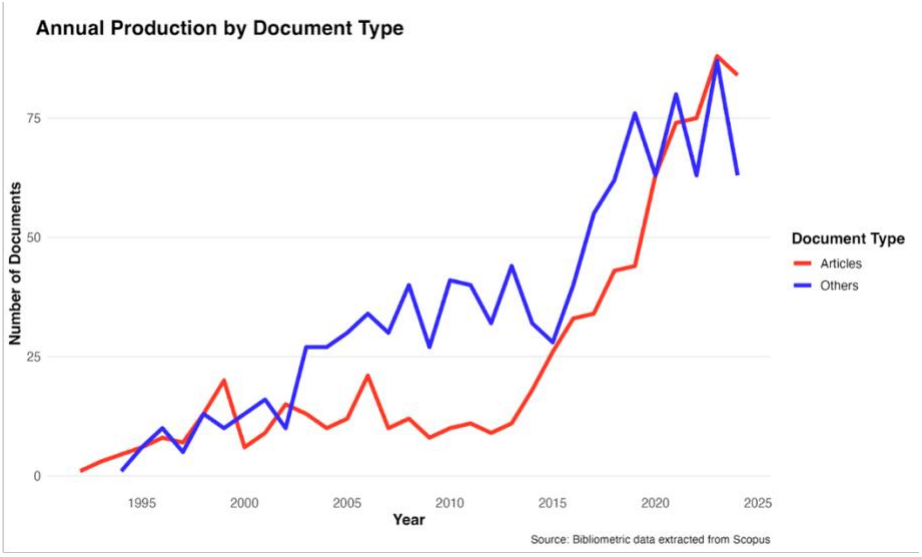
The distribution of document types retrieved (Figure 4) shows that the topic is more commonly addressed in sources other than peer-reviewed journal articles, which make up only 42.1% of the total. Although the Scopus database also indexes books and conference proceedings, only peer-reviewed journal articles were selected for qualitative analysis. This choice reflects both the limited availability of full texts in other formats and the greater academic relevance of journal articles, as indicated by citation frequency.

Figure 10.4: *Distribution of documents by type.*



Concerning changes in publication trends over time, Figure 5 shows a continuous and accelerated increase in the number of published articles from around 2012–2013 onwards. The first reports on Stuxnet emerged in 2010–2011 (Lindsay, 2013), Edward Snowden's revelations became public in June 2013 (Greenwald & Macaskill, 2013), and the initial Russian cyber campaigns against Ukraine took place in 2013–2014—when Russian hackers targeted Ukrainian institutions during negotiations regarding possible EU accession—and again in 2015–2016, when cyberattacks on Ukraine's power grid caused blackouts, including in Kyiv (Devanny, Goldoni, & Medeiros, 2022).

Figure 10.5: *Annual production by document type (1990–2024).*



It was initially hypothesized that the fluctuations in the "other" category might reflect the occurrence of biennial conferences, as similar peaks and troughs appear between 2005–2015 and 2020–2024. However, a closer examination of the conference data did not support this assumption. Most conferences address broader topics and typically contribute only two or three relevant articles each. The diversity of conferences observed, with no single recurring event accounting for the variations, suggests that these fluctuations—more clearly illustrated in Figure 6—are better explained by the incidental nature of contributions rather than a regular publication cycle.

Figure 10.6: *Annual growth rate of scientific production (1994–2024).*

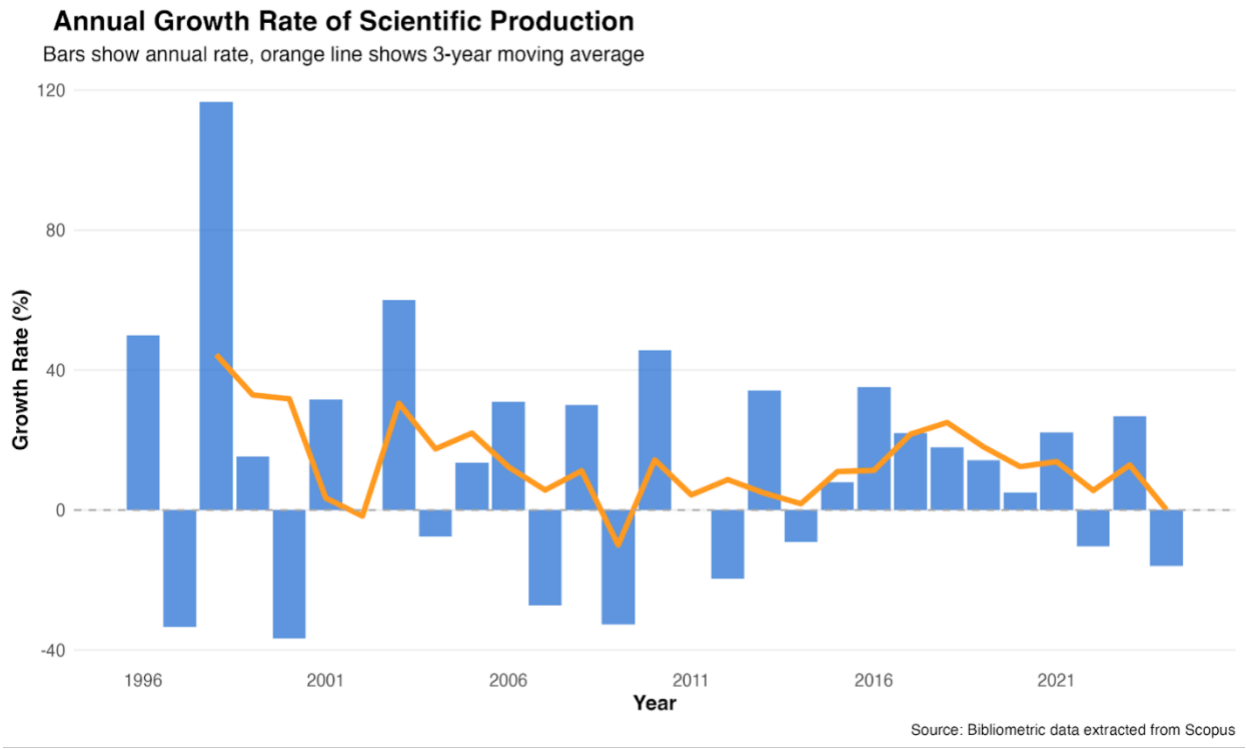


Figure 7 illustrates a significant and sustained increase in scientific publications on the topic. Until 2002, the number of scientific articles and other types of documents followed a similar trajectory. However, the steeper growth curve associated with books, book chapters, and conference proceedings may suggest, on one hand, a growing number of conferences and edited volumes engaging with the subject, and on the other, reflect dynamics within the academic publishing market, particularly concerning journals indexed in the Scopus database.

Figure 10. 7: *Cumulative scientific production (1990–2023).*

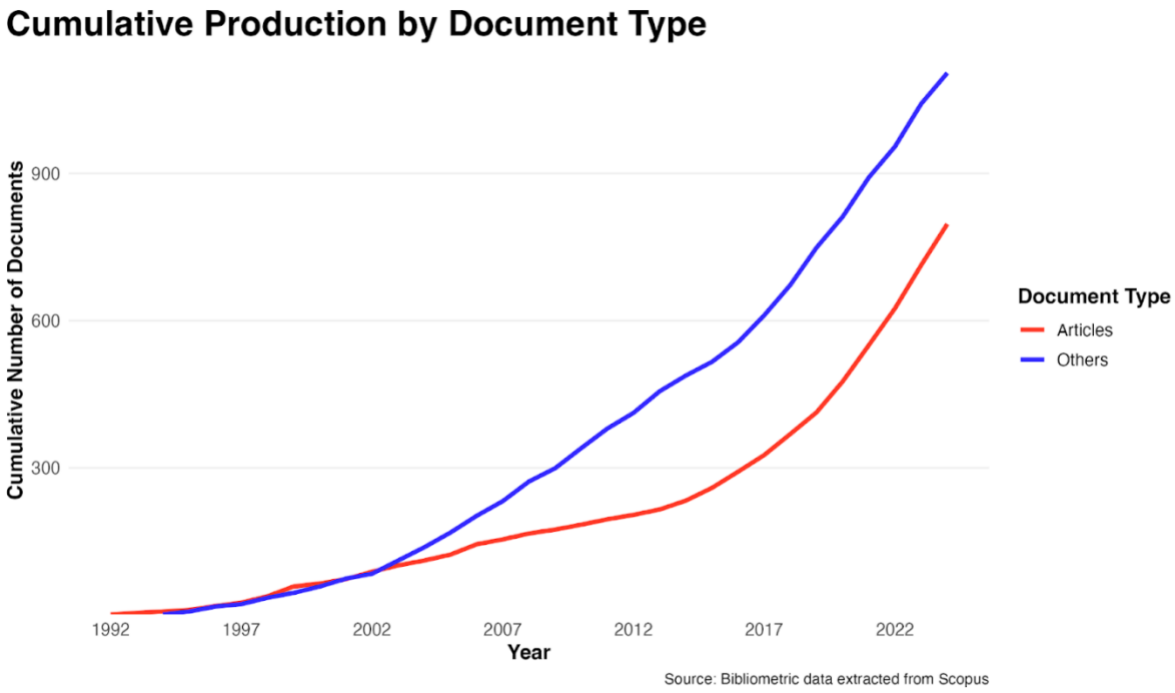


Figure 8 shows that, although journal articles represent only 42.1% of total publications on the topic, they are the most frequently cited and, therefore, can be considered the most academically impactful sources. Articles published between 1996 and 2018 received an average of 12 citations—nearly twice the average of other document types in the same period. The decline in citations for articles published from 2019 onwards likely reflects the time required for academic consolidation and publication cycles, as articles typically take one or more years to be published. This effect may, however, be offset by a growing trend towards citing more recent works. Notably, Figure 9 shows that one of the most cited articles was published in 2019, suggesting that the increasing volume of articles (as shown in Figure 5) may also dilute average citation counts. Figure 9 illustrates the exponential growth in total citations over time, while Figures 10 and 11 offer additional insights into these trends.

Figure 10. 8: *Average citation count by publication year.*

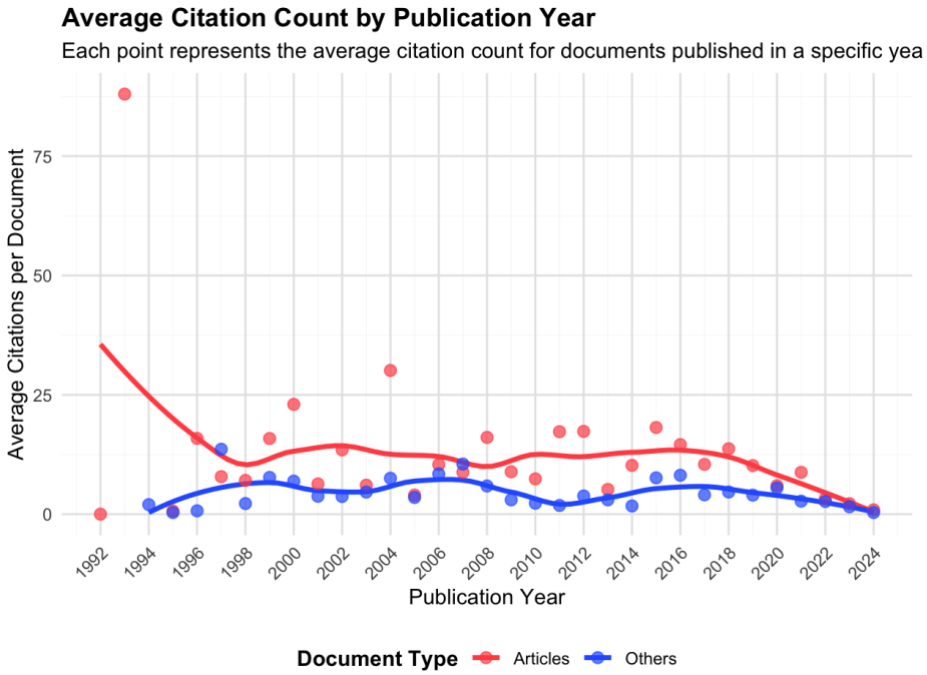


Figure 10. 9: *Cumulative citations over time (1990–2024).*

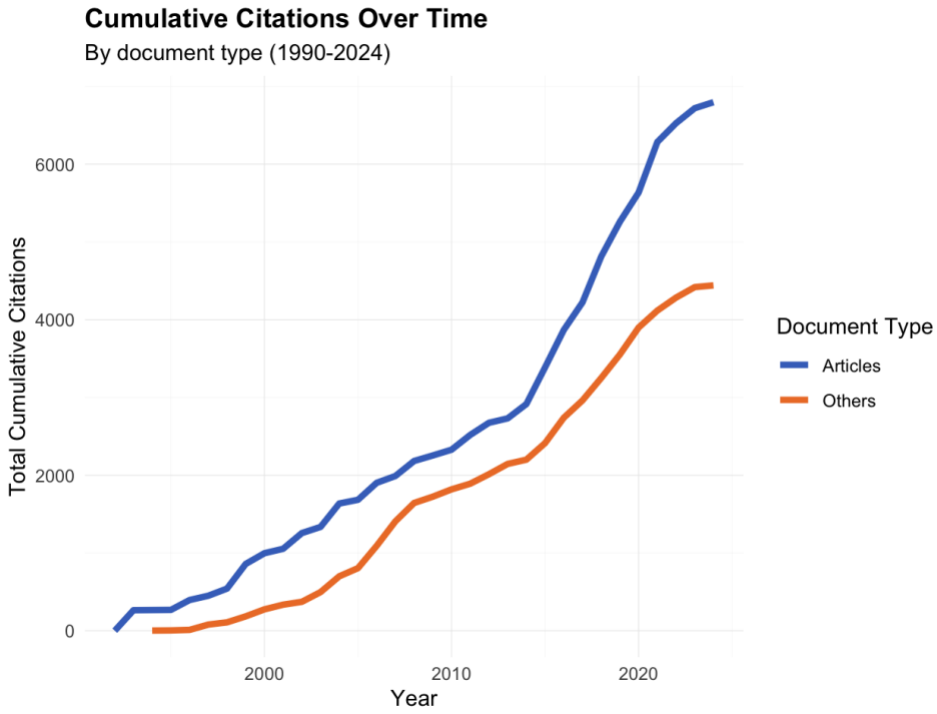


Figure 10 illustrates the rise in both publications and citations of books, book chapters, and conference proceedings over time. Between 1995 and 2005, these document types received

limited attention, with few publications and low citation counts. A notable increase in output is observed in recent years. The most cited documents were published in 2007, 2016, 2018, 2019, and 2020. The scarcity of citations for works published up to 2005, combined with the fact that four of the five most cited years fall within the past decade (2015–2025), suggests a shift in the academic agenda.

Figure 10.10: *Relationship between output and citations: other document types*

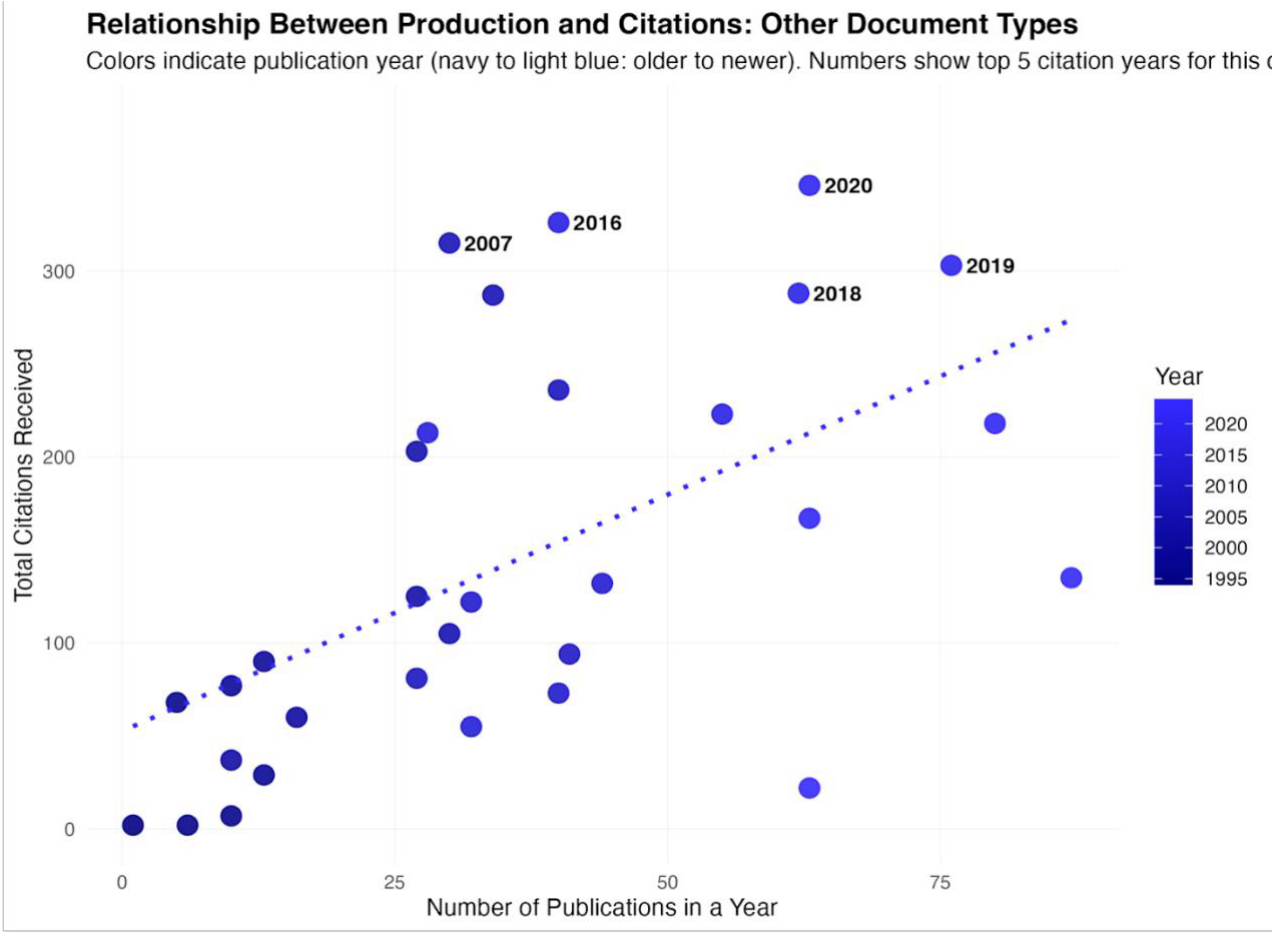


Figure 11 reinforces this trend, showing that the most cited journal articles were published between 2015 and 2021. These patterns indicate that the topic has gained momentum within the social sciences, possibly driven by events such as electoral manipulation in cases like Brexit and the U.S. election, growing tensions with Russia (a state frequently associated with expertise in the area), and the widespread use of social media along with a deeper understanding of its potentially harmful effects.

Figure 10.11: *Relationship between output and citations: articles.*

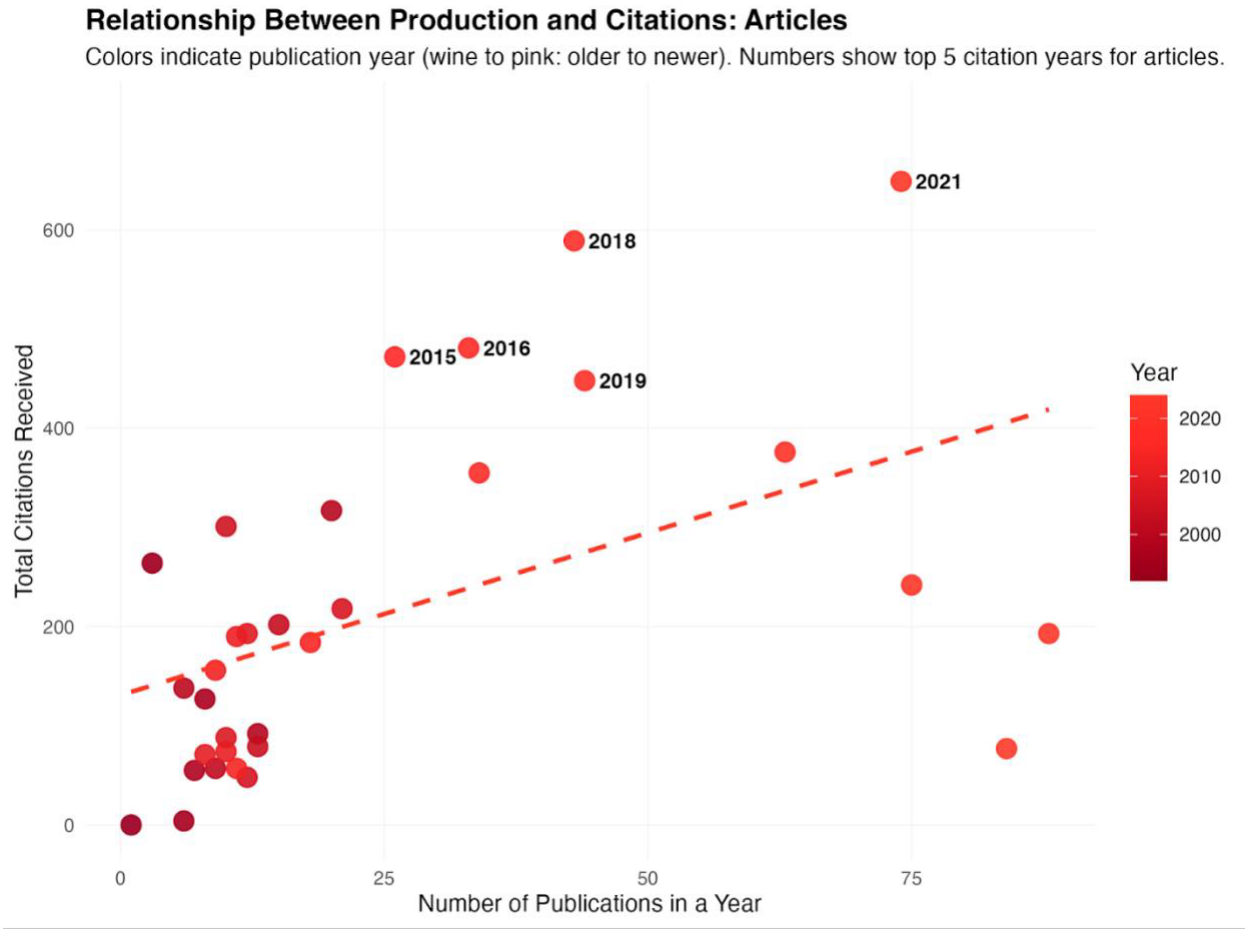
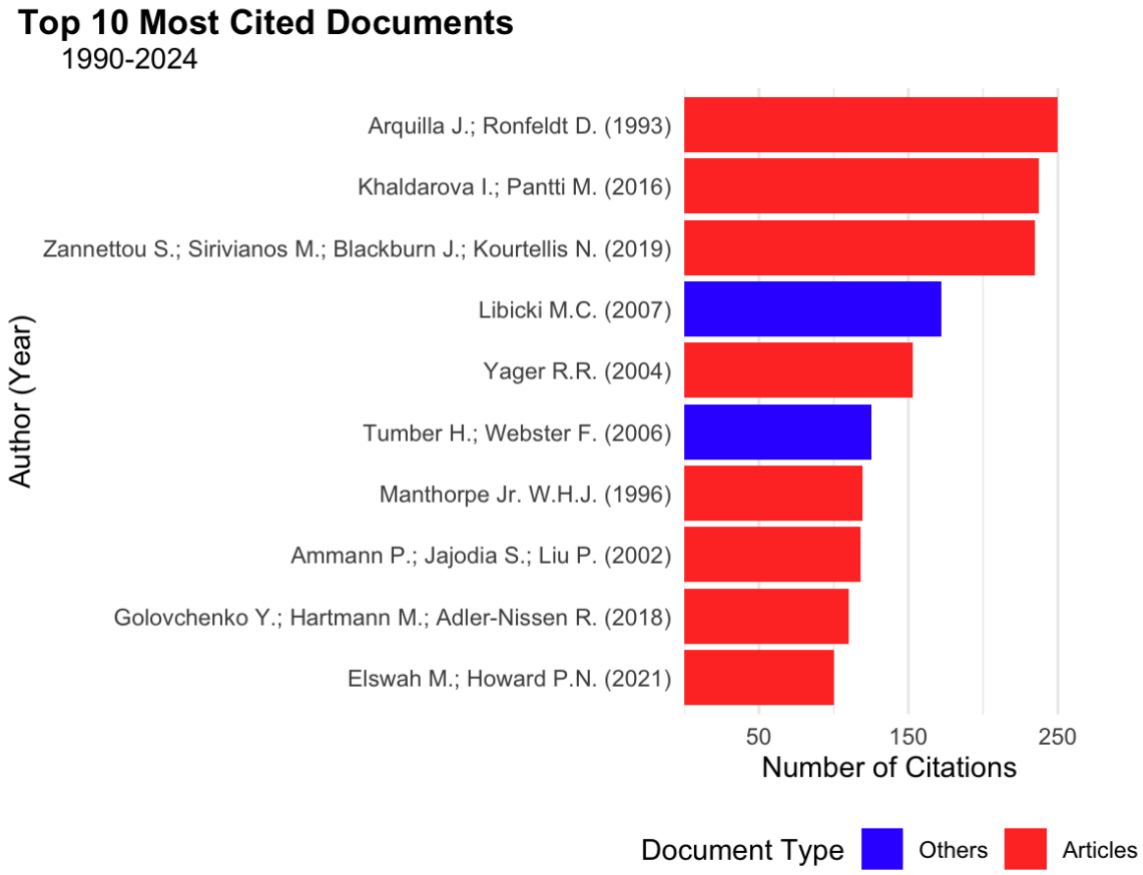


Figure 12 shows that four of the ten most cited documents were published between 2016 and 2021, including two of the top three. Aside from the seminal works of Arquilla and Ronfeldt (1993) and Manthorpe Jr. (1996), all highly cited documents date from the 21st century. Moreover, only two of the top ten are not academic journal articles, underscoring the influence of peer-reviewed articles in research on this topic.

Figure 10.12: *Top-cited documents based on citation count.*



Figures 13, 14, and 15 reveal that high publication output does not necessarily correlate with high citation impact. None of the 20 most prolific authors (Figure 13) appears among the most cited (Figure 14). Furthermore, only five of the 20 most cited authors also feature in the list of those with the highest average citations across at least three articles: S. Jajodia, P. Ammann, J. Arquilla, A. Karatzogianni, and F. Webster (Figure 15). These findings reflect not only the challenge of achieving academic relevance in a particular field, but more crucially, of maintaining that relevance over time. In this sense, they help identify those authors who may be regarded as the most influential in the area—those whose work constitutes essential reading on the subject.

Figure 10.13: *Top 20 most frequent authors by number of publications.*

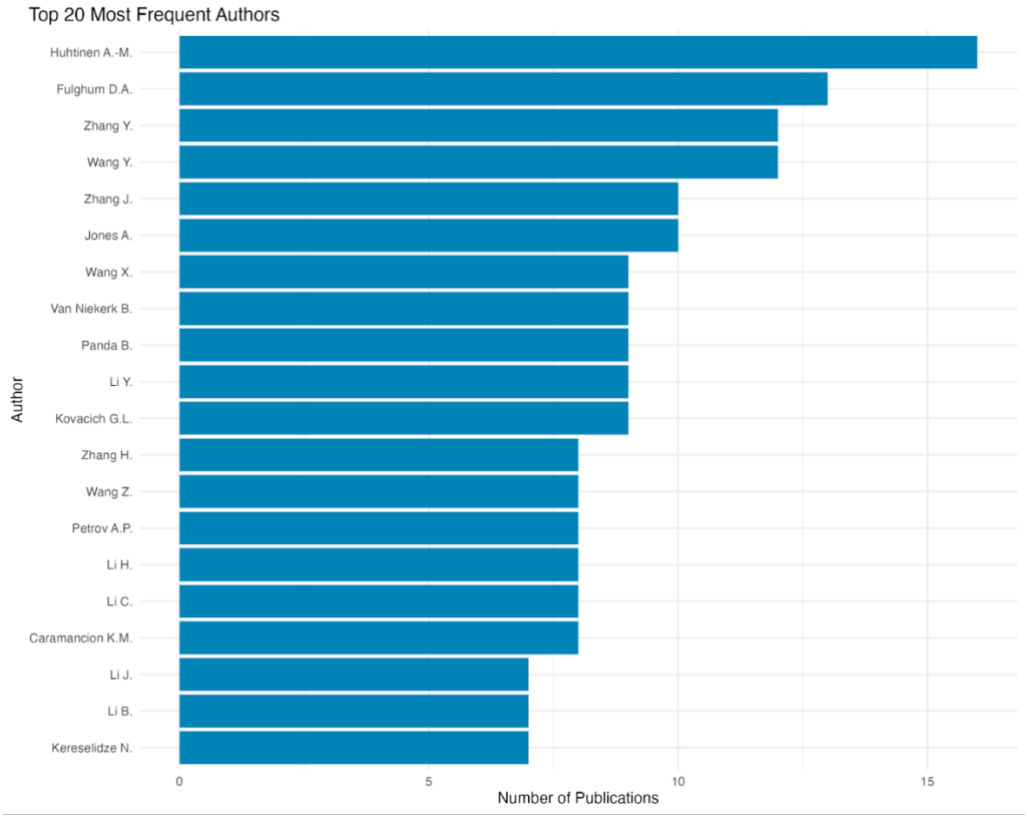


Figure 10.14: *Top-cited authors based on total citations.*

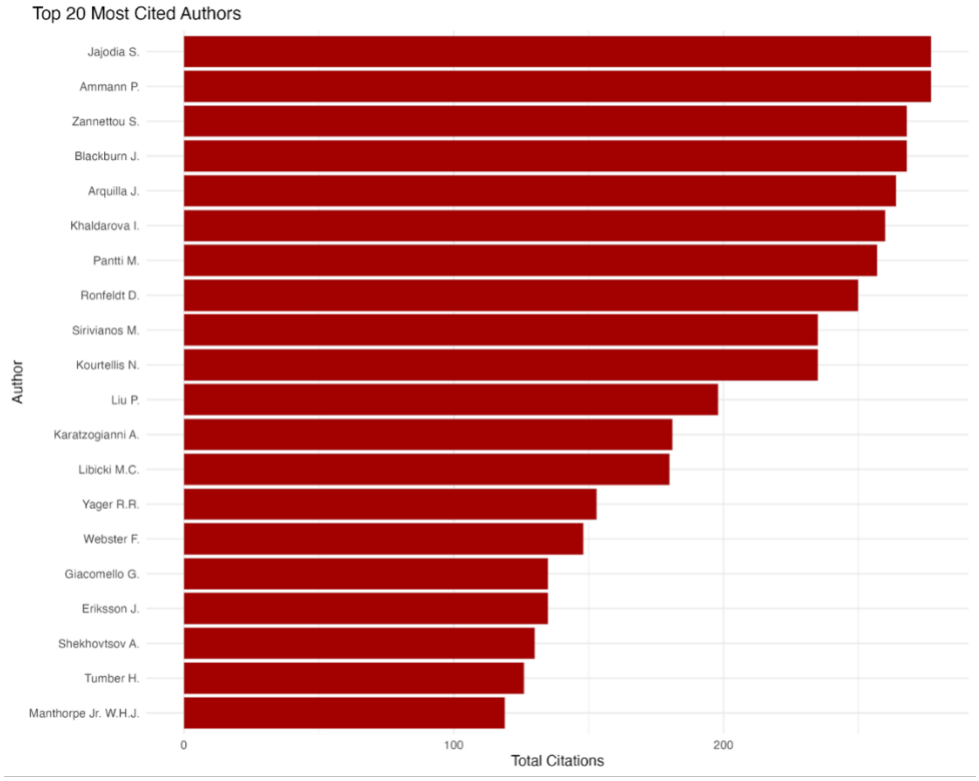
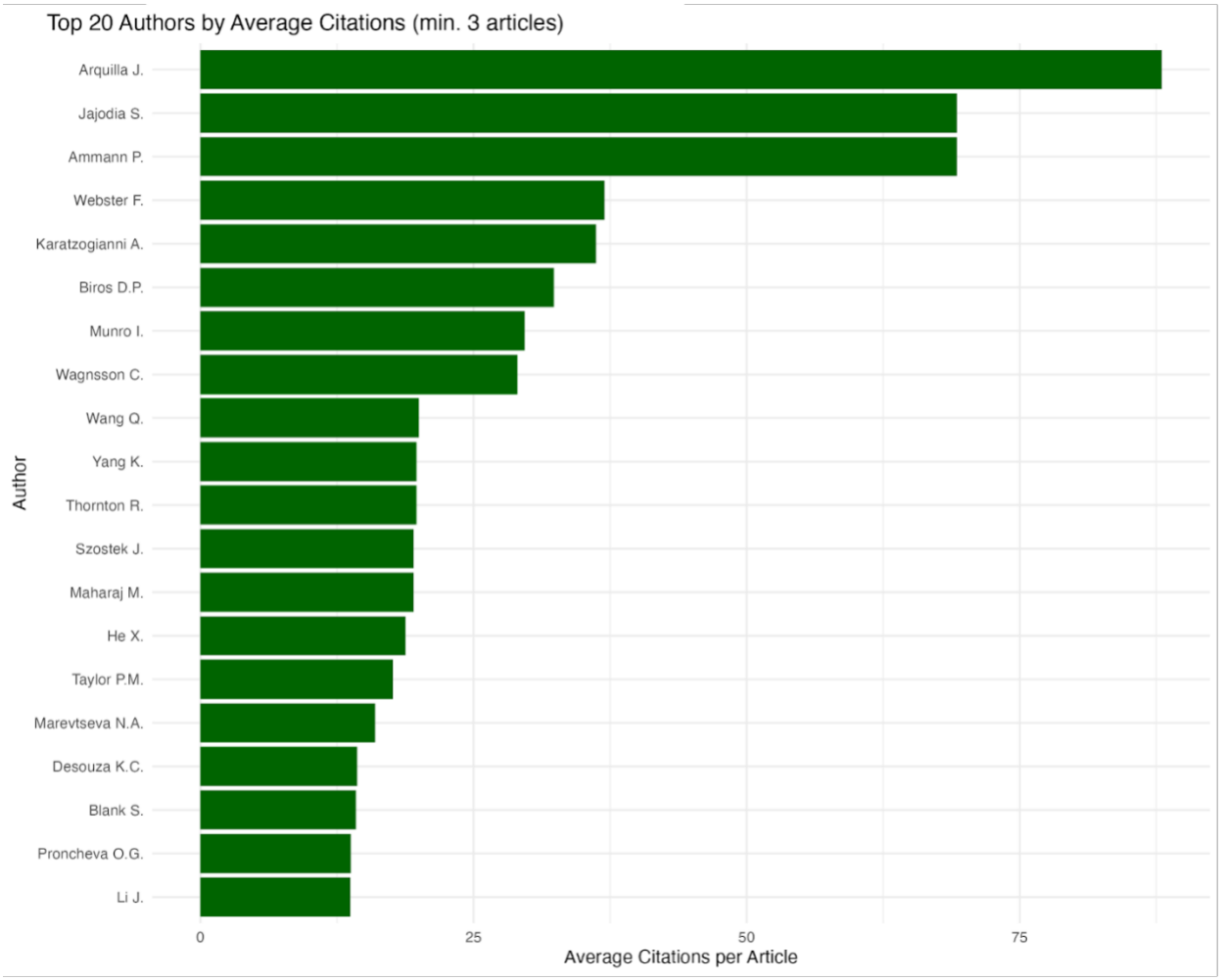
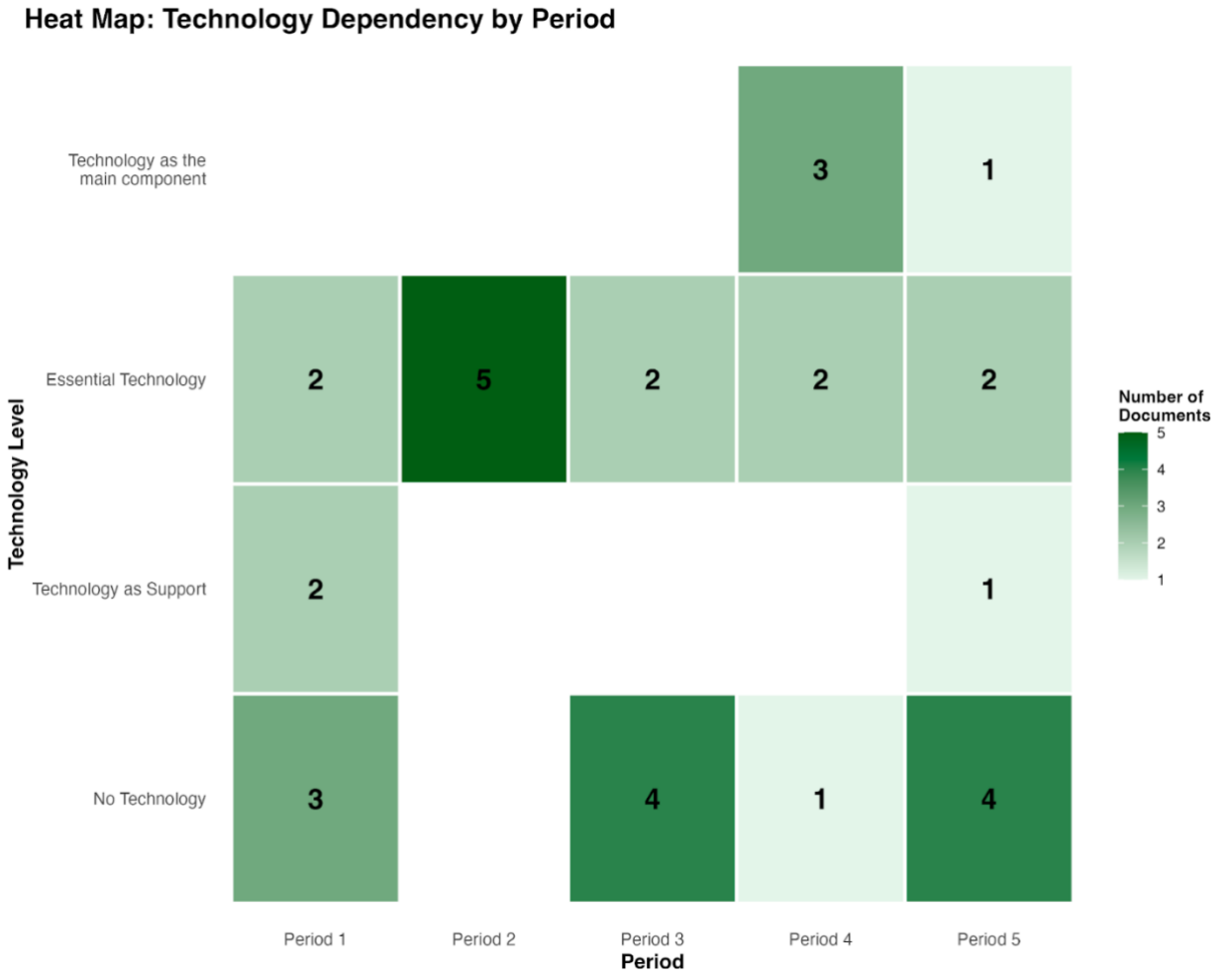


Figure 10.15: *Top-cited authors based on average citations per article.*



After examining how publications on the topic have evolved over time, we now turn to the analysis of how the 32 selected journal articles address the categories of “technological dependency,” “destinatary,” and “target.” Figure 16 shows that 12 out of the 32 articles (37.5%) either do not mention technology or consider it only marginally relevant. In contrast, 13 articles (40.6%) describe technology as essential to the analysis. In four articles, technology is identified as the central element. Together, these findings suggest that over half of the articles (53%) see technology as either essential or the main component.

Figure 10.16: *Technology Dependency by Period.*



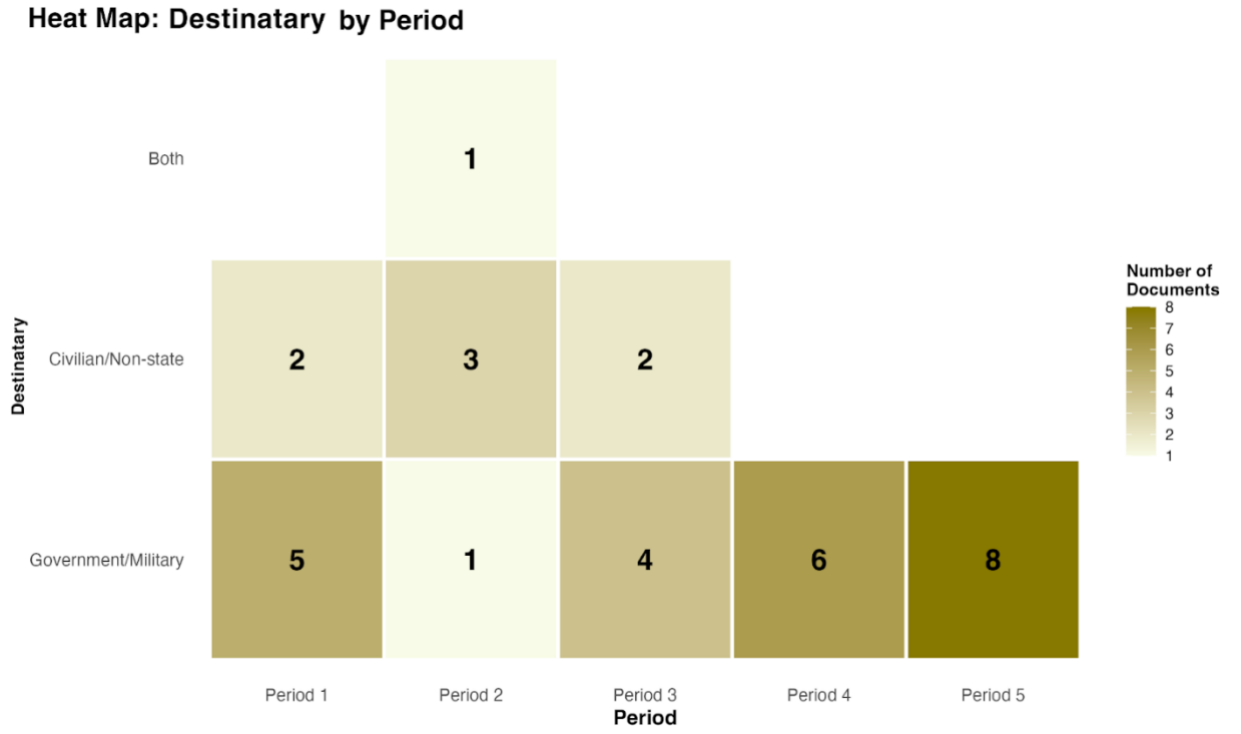
Across the five periods, there is a consistent number of articles—two per period—that describe technology as essential, except for Period 2, which has five. Articles that identify technology as the main component appear only in Periods 4 and 5. This may reflect a growing scholarly awareness of the role of digital platforms such as social media, smartphones, apps like Discord and Roblox, and targeted advertising and other innovations, in reshaping information flows.

When counting all articles that present technology as supportive, essential, or central (P1: 4 articles; P2: 5; P3: 2; P4: 5; P5: 5), only Period 3 shows a higher number of articles in which technology is either absent or of little importance. An intriguing pattern emerges: three periods (P1, P3, and P5) in which technological dependency is largely dismissed are interspersed with two periods (P2 and P4) in which it is widely treated as essential or central. Rather than reflecting analytical inconsistencies, this oscillation may illustrate how the field reacts to external events and

technological shifts—highlighting the evolving frameworks through which information warfare is theorized.

Figure 17 shows that, among the 32 articles analysed, 24 (75%) identify society at large as the main destinatary of informational warfare, rather than military targets. Period 2 is the only deviation from this trend, as it includes the sole article in which military targets are the exclusive destinatary, alongside three others where they are targeted in conjunction with the broader population. This aligns with Figure 16, which shows that Period 2 also contains the highest number of articles categorizing technology as an essential element.

Figure 10.17: *Destination by Period.*



This shift in Periods 4 and 5 appears to reflect a conceptual refinement of information warfare. While earlier literature, particularly in Period 2, frequently used the term in association with cyberattacks and concerns about hackers and critical infrastructure, more recent works tend to reserve the concept for operations aimed at shaping public opinion and manipulating collective behaviour. The disappearance of the military as a destination in these later periods does not suggest the end of conventional warfare—tanks and troops are still very much in use—but rather a growing emphasis on the emotional and psychological dimensions of conflict. If the 1990s marked the beginning of anxieties surrounding digital vulnerabilities, the post-2015 period foregrounds the weaponisation of attention, trust, and truth itself.

To assist in analysing both categories together, Figure 18 cross-references technological dependence and destination. It shows that technology is least discussed in articles where society as a whole is a target (Tech 0, Destination 0). Conversely, when military targets are the destination (Destination 1), articles tend to report higher technological dependence (Tech 2), reinforcing the association between military conflict and technological capabilities. In such cases, the objective is not to sway public opinion but to disrupt the functioning of complex, often highly secured systems—an aim that demands a far greater technological infrastructure.

Figure 10.18: *Relationship Tech x Destination.*

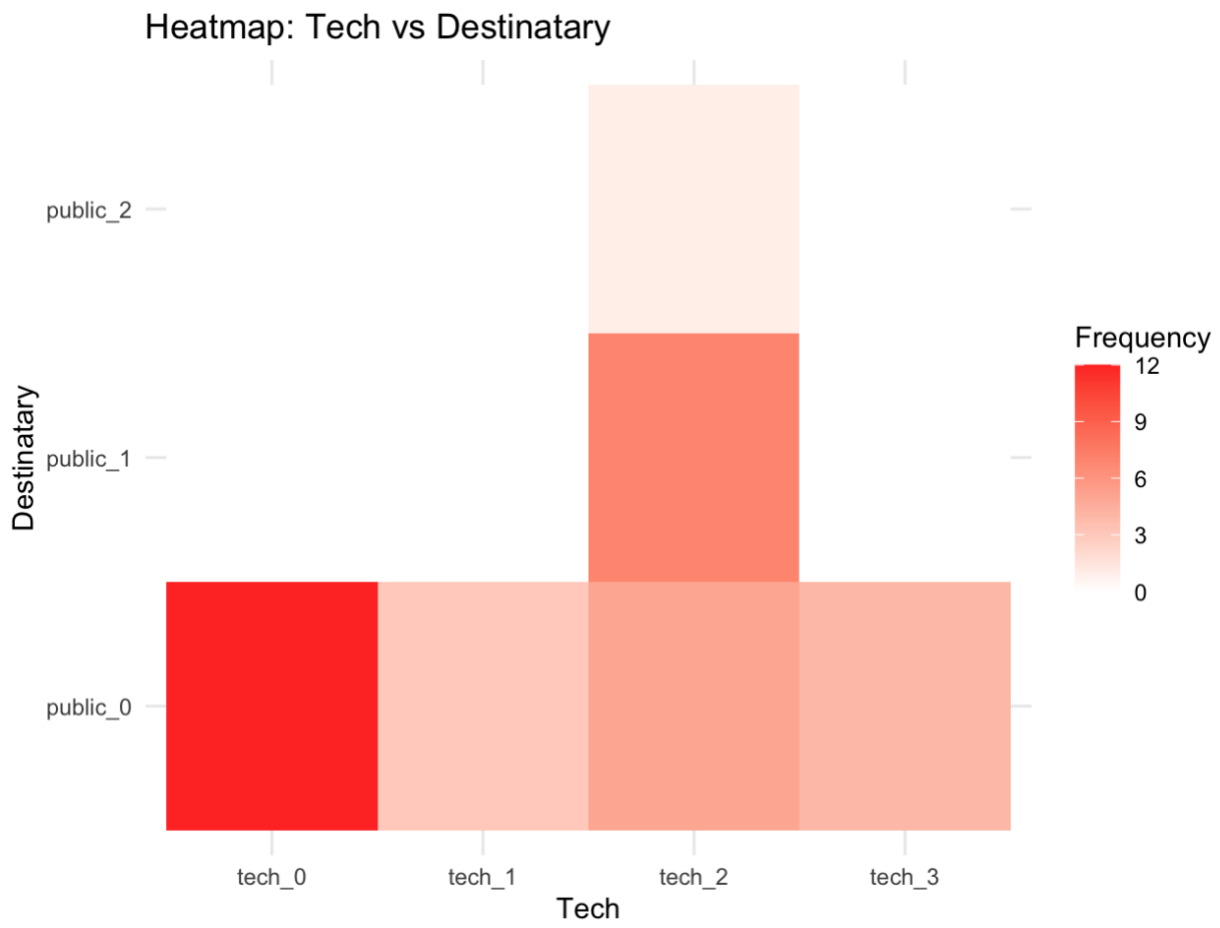


Figure 19 confirms that, within the context of information warfare, the primary target is information itself. Only one of the 32 analysed articles focuses exclusively on systems, suggesting that this type of vulnerability is not central to the literature on the subject – or, if it is, it may be addressed using different terminology. This trend becomes more pronounced in periods 4 and 5, which show a clear concentration of articles identifying information as the main target (P4: 5+1; P5: 6+2, as shown in Figure 19) and society as the main destinatary (P4: 6; P5: 8, as shown in

Graph 17). Figure 20 reinforces this pattern, highlighting a clustering of articles in the Target 0 and Destinatary 0 categories, indicating that the impacts of information warfare fall primarily on civil society – rather than on military structures or technical systems.

Figure 10.19: *Target by Period.*

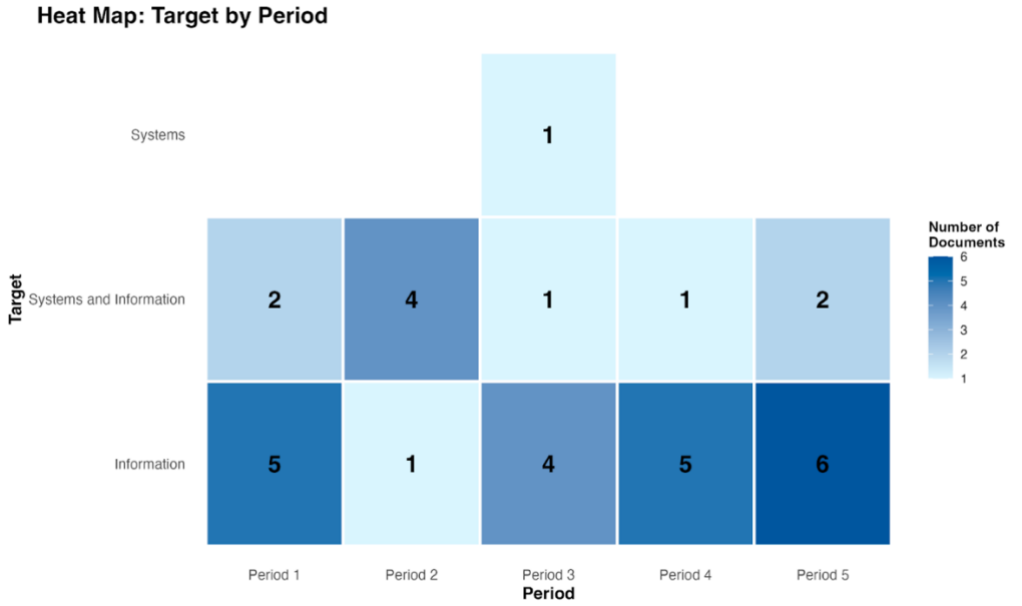


Figure 10.20: *Relationship Destinatary x Target.*

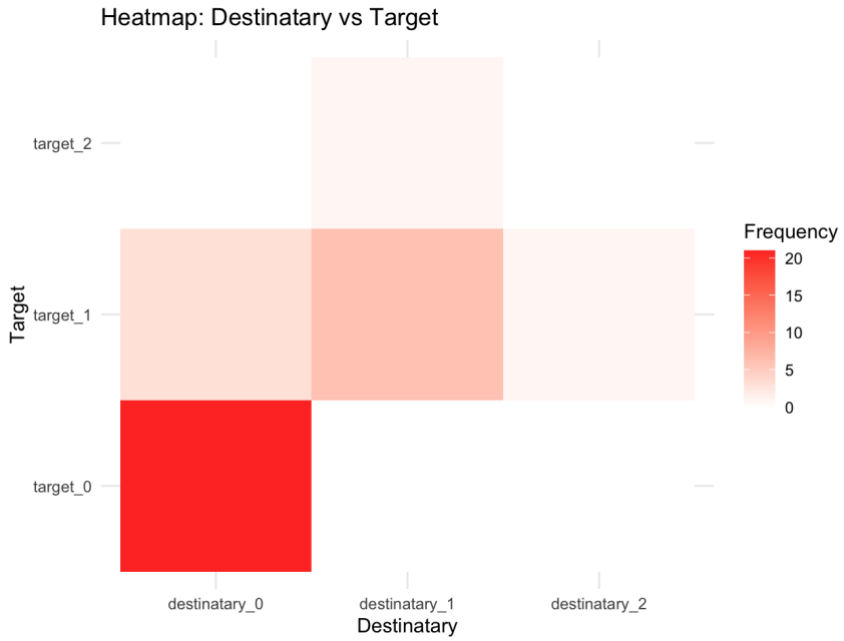
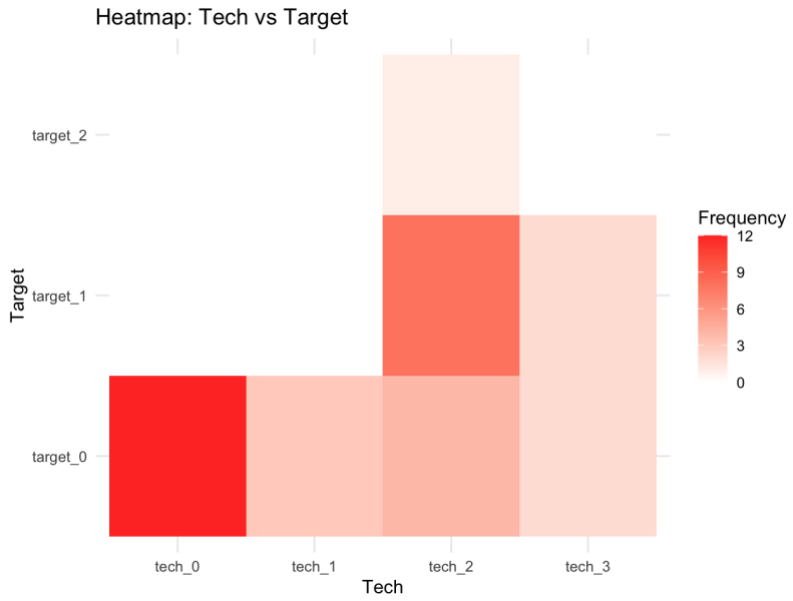


Figure 21, in turn, shows a pattern similar to that observed in Figure 18: the highest concentration of articles falls under Tech 0 and Target 0, followed by Tech 2 and Target 1. In other

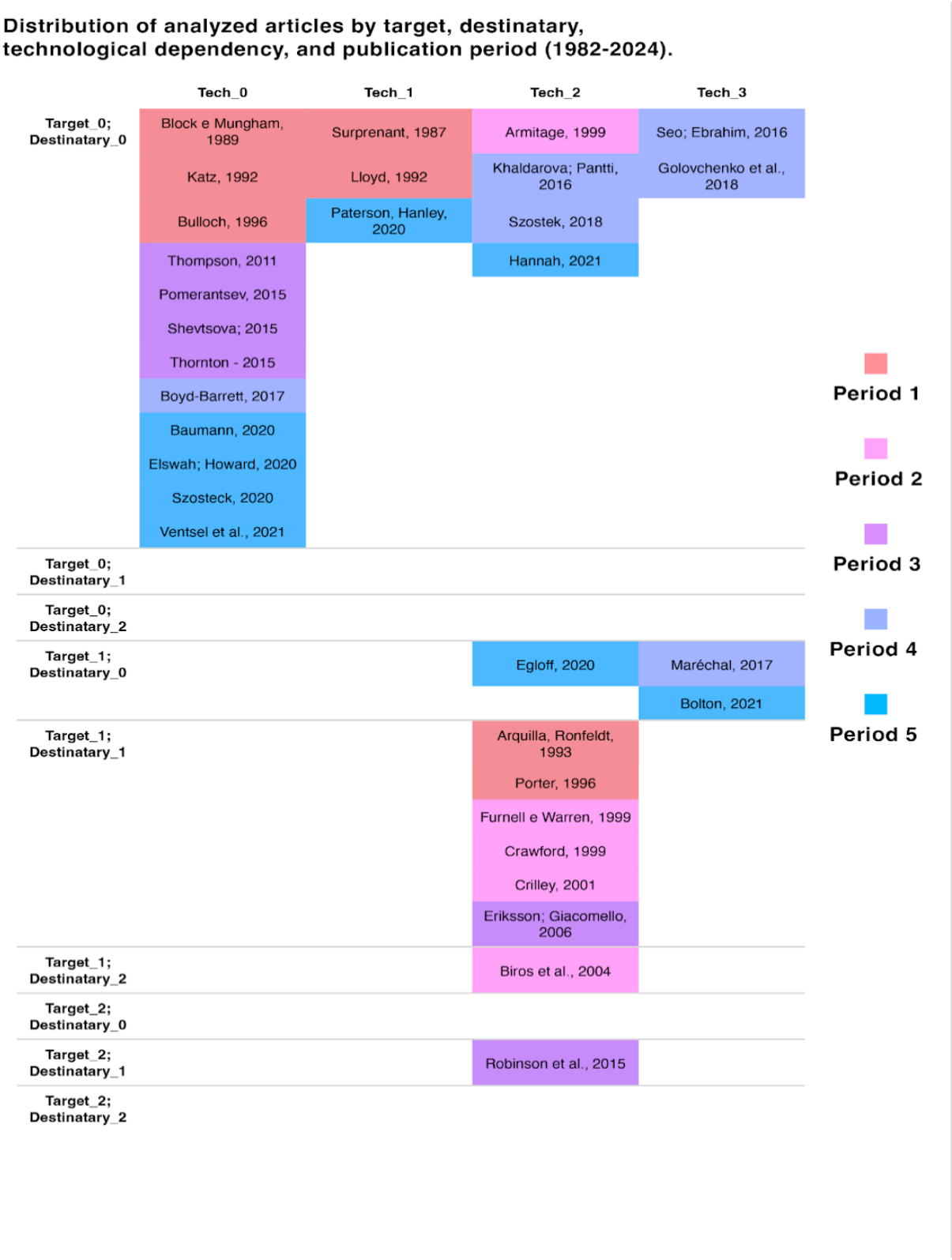
words, most of the analysed articles place little emphasis on technological dependency and identify information as the main target. The second most common group consists of articles that view technology as indispensable and point to both society and the military as targets. These findings are summarized in Figure 22.

Figure 10.21: *Relationship Tech x Target.*



As shown in Figure 22, 21 out of the 32 analysed articles (65.6%) were classified as Target 0 and Destinatary 0 – that is, they identify information as the primary target and society as the main destinatary, excluding systems as targets and military actors as destinataries. Among these 21 articles, 12 were also classified as Tech 0. This may reflect works that focus on information and society at large, while paying little or no attention to technology – or, as outlined in the Methodology, articles with a stronger theoretical emphasis. Conversely, it is worth noting that 13 articles were classified as Tech 2, and of the five most cited articles in the sample, three (Arquilla & Ronfeldt, 1993; Khaldarova & Pantti, 2016; Eriksson & Giacomello, 2006) are classified as Tech 2, and one (Golovchenko et al., 2018) as Tech 3 – that is, they are studies that regard technology as highly important or essential. This may suggest that, although the concept of information warfare does not necessarily refer to digital or contemporary phenomena, studies that engage more directly with such aspects tend to hold greater relevance or recognition within the field.

Figure 10.22: *Distribution of analyzed articles by target, destinatary, technological dependency, and publication period (1982-2024).*



The second highest concentration of articles—six in total—falls under those classified as Target 1, Destinatary 1, and Tech 2. These are studies that regard technology as fundamental, identify both information and systems as targets, and recognize both society and military actors as destinataries. This group includes the most cited article in the dataset (Arquilla & Ronfeldt 1993, with 250 citations) and the fifth most cited (Eriksson & Giacomello 2006). Of the five remaining articles, three were classified as Target 1 and Destinatary 0 (two Tech 3 and one Tech 1), and three as Tech 2, all of which include the military as a target—either exclusively or alongside society.

As for the secondary analysis, only 10 out of the 32 qualitatively analysed articles—roughly one third—make explicit reference to theoretical considerations: P1: 0; P2: 1; P3: 2; P4: 3; P5: 4. This distribution suggests a growing concern with theoretical reflection in recent years, and an increasing sophistication of analyses when compared to earlier periods, which were more focused on empirical observations and forecasting trends. Among the theoretical frameworks cited are phenomenology (Armitage, 1999), realism and liberalism (Eriksson, 2006), constructivism (Eriksson, 2006; Ventsel et al., 2021), post-structuralism (Bauman, 2020), ontological security (Bolton, 2021), and grounded theory (Boyd-Barret, 2017; Seo & Ebrahim, 2016).

Regarding methodology, a similar proportion of articles explicitly present the research method(s) employed—11 out of 32 in total: P1: 0; P2: 2; P3: 0; P4: 6 (all analysed); P5: 3. This evolution suggests an increase in the degree of scientific rigour in research on the topic, which may stem from broader changes in academic training and research practices, improved access to empirical research tools through new technologies, or shifts within the field itself. Among the methodologies employed are systematic data collection (Robinson, Jones, & Janice, 2015), content analysis of reports published in mainstream newspapers (Bauman, 2020; Boyd-Barret, 2017; Ventsel et al., 2021), interviews (Elswah & Howard, 2020; Szostek, 2018), and social network analysis (Golovchenko, 2018; Khaldarova, 2016; Seo & Ebrahim, 2016).

Furthermore, there was a high frequency of references to "propaganda" (14 articles), "values" (10 articles), "public opinion" (15 articles), "media" (16 articles), and "information control" (21 articles), indicating a strong emphasis on the communicational and symbolic dimensions of information warfare. The term “contemporary Russia” appeared in 10 articles, reflecting the country’s central role in current debates on the topic. Notable mentions also include the use of information warfare in support of conventional conflicts (6 articles) and cyberattacks (11 articles). These findings reinforce the centrality of narrative contests, the strategic manipulation of information, and the integration of digital and conventional means as defining features of contemporary information warfare practices.

Final Remarks

In this chapter, we sought to understand where, by whom, how, and in what ways academic literature has approached, interpreted, and analysed information war/warfare. Rather than proposing fixed definitions or distinguishing between what is right or wrong, our aim was to identify the most recurrent and consolidated approaches within scholarly debates.

The fact that only one of the articles analysed considers the system itself as the target of information warfare does not invalidate this perspective — on the contrary, it underscores the interpretative diversity surrounding the topic and points towards alternative analytical paths that warrant further attention. Such plurality is particularly valuable in a field that is still in the process of consolidation.

It is worth noting that all articles reviewed were published in recognized academic journals and underwent formal peer-review processes, thereby meeting the quality standards expected within their respective disciplines. Despite conceptual and methodological divergences, these works constitute meaningful contributions that have, directly or indirectly, shaped the contours of current academic debates.

Furthermore, we observed what may be interpreted as a process of refinement — or even redefinition — within the scholarly field concerned with information warfare. Initially characterised by a broader scope, often encompassing activities such as cyberattacks and technical interference, the concept has increasingly come to be associated with narrative disputes, symbolic manipulation, and informational control. This shift suggests not only changes in the practices under analysis, but also in the theoretical and methodological frameworks employed by researchers.

In addition, we identified a significant diversity of perspectives regarding the centrality of technology in this phenomenon. While some articles give little to no consideration to the technological dimension, others treat it as a foundational component of information warfare. This lack of consensus reflects not only the complexity of the subject, and the variety of analytical lenses applied, but also the multiplicity of strategies that coexist within a competitive international environment — one in which different paths are pursued in the quest for influence and power. This reality reinforces the importance of comparative and interdisciplinary approaches in future research.

This mapping also highlights how asymmetries in global knowledge production may reflect or reinforce the capacity and willingness of certain actors to shape the information environment. Regions or institutions that dominate the academic debate may have greater resources not only to theorize information warfare, but also to deploy and counter such strategies in practice.

Recognizing these disparities suggests the need for further comparative studies that examine how different contexts influence both the practice and the study of information warfare.

The taxonomy proposed here can also serve as a practical tool for analyzing current information campaigns. For example, it may help distinguish and compare the multiple strategies employed by actors such as Russia in its post-2022 operations—ranging from overt propaganda and disinformation to more subtle forms of narrative shaping and technological disruption. By clarifying these categories, the taxonomy contributes to a more precise understanding of how diverse tactics coexist and interact in contemporary conflicts.

Lastly, it should be noted that this analysis did not examine the nature of the citations of the selected articles — whether positive, critical, or neutral — nor did it assess their lasting impact over time. These remain open questions, particularly regarding the real influence of such works on the consolidation of a scholarly field still in formation. These gaps offer fertile ground for future investigations that not only expand the scope of this research but also shed light on how academic consensus, controversy, and silence are formed in relation to information warfare. Understanding how academia structures its debates on information warfare is also to understand the intellectual foundations that shape policy decisions, strategic doctrines, and broader public perceptions of the issue.

References

Abusaada, H., & Elshater, A. (2022). Notes on Developing Research Review in Urban Planning and Urban Design Based on PRISMA Statement. *Social Sciences*, 11(9), 391. https://doi.org/10.3390/socsci11090391

Baldwin, D. A. (1997). The Concept of Security. *Review of International Studies*, 23(1), 5–26. https://doi.org/10.1017/S0260210597000053

Bornmann, L., & Daniel, H. D. (2008). What Do Citation Counts Measure? A Review of Studies on Citing Behavior. *Journal of Documentation*, 64(1), 45–80.

Bourdieu, P. (1989). *O Poder Simbólico*. Bertrand Brasil.

Castells, M. (1999). *A Sociedade em Rede: A Era da Informação – Economia, Sociedade e Cultura*. Paz e Terra.

Devanny, J., Goldoni, L. R. F., & Medeiros, B. P. (2022). Strategy in an Uncertain Domain: Threat and Response in Cyberspace. *Journal of Strategic Security*, 15(2), 34-47.

Foucault, M. (2002). *The Archaeology of Knowledge*. Routledge.

Fuller, J. F. C. (2002). *A Conduta da Guerra* (2nd ed.). Biblioteca do Exército Editora.

Greenwald, G., & Macaskill, E. (2013). NSA Prism program taps in to user data of Apple, Google and others. *The Guardian*.

Hall, S. (1997). The Work of Representation. In S. Hall (Ed.), *Representation: Cultural Representations and Signifying Practices*. SAGE.

High, A. C., Ruppel, E. K., McEwan, B., & Caughlin, J. P. (2023). Computer-Mediated Communication and Well-Being in the Age of Social Media: A Systematic Review. *Journal of Social and Personal Relationships*, 40(2).

Keegan, J. (1996). *Uma História da Guerra*. Companhia das Letras.

Latour, B., & Woolgar, S. (1997). *A Vida de Laboratório: A Produção dos Fatos Científicos*. Relume Dumará.
Liberati, A., Altman, D. G., Tetzlaff, J., Mulrow, C., Gøtzsche, P. C., Ioannidis, J. P. A., Clarke, M., Devereaux, P. J., Kleijnen, J., & Moher, D. (2009). The PRISMA statement for reporting systematic reviews and meta-analyses of studies that evaluate health care interventions: Explanation and elaboration. *Journal of Clinical Epidemiology*, 62(10), e1–e34. https://doi.org/10.1016/j.jclinepi.2009.06.006
Liddell Hart, B. H. (2010). *As Grandes Guerras da História* (6th ed.). IBRASA.
Lindsay, J. R. (2013). Stuxnet and the Limits of Cyber Warfare. *Security Studies*, 22(3), 365–404.
Marsili, M. (2023). Hybrid Warfare: Above or Below the Threshold of Armed Conflict? *Honvédségi Szemle*, Nr. 1–2. https://doi.org/10.5281/zenodo.7557494.
Nye, J. S. (2011). *The Future of Power*. PublicAffairs.
Saldaña, J. (2013). *The coding manual for qualitative researchers* (2nd ed.). SAGE.
Santos, M. (2017). *Toward an Other Globalization: From the Single Thought to Universal Conscience* (Vol. 12). Springer International Publishing. https://doi.org/10.1007/978-3-319-53892-1.
SCImago. (2025). SJR — SCImago Journal & Country Rank [Portal]. Retrieved April 1, 2025 from https://www.scimagojr.com.
Skinner, Q. (1969). Meaning and Understanding in the History of Ideas. *History and Theory*, 8(1), 3–53.
Singh, V. K., Singh, P., Karmakar, M., Leta, J., & Mayr, P. (2021). The journal coverage of Web of Science, Scopus and Dimensions: A comparative analysis. *Scientometrics*, 126(6), 5113–5142. https://doi.org/10.1007/s11192-021-03948-5
Stritzel, H. (2014). *Security in Translation: Securitization Theory and the Politics of Translation*. Palgrave Macmillan.
Sun Tzu. (2010). *The Art of War*. Apple Books Classic.
Taylor, C. (1985). *Philosophy and the Human Sciences*. Cambridge University Press.
Thucydides. (2009). *The History of the Peloponnesian War*. Apple Books Classic.
Vaismoradi, M., Turunen, H., & Bondas, T. (2013). Content analysis and thematic analysis: Implications for conducting a qualitative descriptive study. *Nursing & Health Sciences*, 15(3), 398–405. https://doi.org/10.1111/nhs.12048
Williams, M. C. (2007). *Culture and Security: Symbolic Power and the Politics of International Security*. Routledge.
Wittgenstein, L. (2009). *Philosophical Investigations*. Blackwell Publishing.
Zhang, X., & Lin, W. Y. (2023). Exploring Information Dissemination Effect on Social Media: An Empirical Investigation. *Personal and Ubiquitous Computing*, 27(4).
Yu, Y., Jin, Z., & Qiu, J. (2021). Global Isotopic Hydrograph Separation Research History and Trends: A Text Mining and Bibliometric Analysis Study. *Water*, 13(18), 2529. https://doi.org/10.3390/w13182529.

Chapter 11: The Significance of News as an Aspect of Information Operation in the South China Sea Conflict

Dr. Bagus **Jatmiko**, ORCID: https://orcid.org/0000-0002-1092-2602
Prof. Dr. **Marsetio** ORCID: https://orcid.org/0009-0006-3935-8853

Dr. Irhamni **Ali** ORCID: https://orcid.org/0000-0002-3715-4244

Abstract:

This study aims to investigate the impact of news and media outlets as a strategic aspect of information operations and warfare in the South China Sea (SCS) conflict. This chapter article assumes that news media are used as the conduit for information operations (IO) in narrative construction and perception management towards the conflict. This study investigates the mainstream news outlets to examine their influence on the evolving narratives of the SCS conflict through the dissemination of disinformation and misinformation. This studyuses descriptive in combination with sentiment analysis, Exploratory Data Analysis (EDA), Latent Dirichlet Allocation (LDA), Time Series Analysis, and Trigram Analysis through information extraction from the news database. Furthermore, it highlights the interplay between news reporting and information operation to reveal the fact presentation, events framing, and propagation of certain storylines that serve as tools for shaping public opinion and international discourse on the issue of the conflict. The findings of this study show that the media is an effective means of shaping public perception, providing insights into the potential and interesting utilization of media as an aspect of information operations in modern conflict dynamics, taking the case of the SCS conflict. It underscores the need for critical media literacy and advocates for a balanced approach to news consumption in an era where information and data can be used as both weapons and currency. Moreover, this study offers an alternative analysis method for investigating the phenomenon of disinformation and misinformation utilization in information operations or even warfare.

Keywords: Information operation, information warfare, disinformation, misinformation, narrative building, South China Sea

Introduction

This study focuses on the conflict in the South China Sea [SCS] region, a contemporary conflict that is characterized by a complex interplay of kinetic and non-kinetic strategies. Kinetic strategy is defined as a traditional form of strategy that emphasizes the use of physical force and direct combat to achieve strategic objectives that grounded mainly in military power (Teo, 2008), including deploying military assets, building artificial islands, and also using militia as proxies to conduct aggressive maneuvers (Kania, 2016). Meanwhile, non-kinetic strategies are mainly defined as the use of non-physical means to achieve military objectives, including informational, psychological, diplomatic, economic, social, and technological tools of statecraft to achieve national interests and objectives (Lehto & Henselmann, 2020).

The nature of the gray zone conflict in the SCS affects how countries deploy their strategies on regional issues, which this study assumes would be a mix of kinetic and non-kinetic strategies. Nevertheless, the non-kinetic strategies have come forward to complement the kinetic ones. A gray zone is defined as a condition that cannot be included under the category of peace or war but is somewhere in between and is below the threshold of open military conflict (Bueger, 2020; Guan & Koh, 2022). In the SCS, China is infamously deploying its non-kinetic "three warfares" strategy, which includes psychological, media, and legal warfare (Martin, 2021). This strategy aims to influence perceptions and behaviors to achieve strategic objectives with minimal or without direct military confrontation. Among these three aspects of the strategy, this study focuses on the use of media as a means to conduct information operations or warfare. This study assumes that the other countries in the region also utilize media as the means to galvanize support in favor of their respective national agendas, particularly related to the narrative of the SCS conflict. This inference is made from the fact that China focuses on the use of media in its three warfares strategy and the finding on media anomaly due to international legal decisions in shaping media narratives and public discourse on territorial disputes. Hence, the analysis conducted in this study is not restricted to certain countries in the region but focuses more on the elaboration of the pattern of media use in information operations in the SCS conflict.

Research Question and Methods

This study is taking the research question of "What is the pattern of media utilization for information operations in the SCS conflict?" In dealing with the question, this study takes the assumption that the countries in the region are using media outlets for information dissemination to support their respective agendas related to the regional conflict. Moreover, this paper proposes the combination of descriptive analysis of the extant literature on the use of information operations and warfare with the exploratory topic analysis and sentiment analysis of the news information extracted from the open-access LexisNexis news database, particularly in relation to the SCS conflict (Ali & Jatmiko, 2024). This study analyzes the media using English as the main language of publications. Hence, news in other languages is not included. These methods are meant to reveal the sentiment inclination of news or media information toward the issue of the SCS conflict (Wankhade et al., 2022). More specifically, this paper highlights the role of news reporting in information operations that serve as tools for herding, shaping public opinion, and building certain narratives in support of specific political agendas.

This study collected news articles using several keywords. The keywords used were Information Operation AND South China Sea, Information Operation AND South China Sea,

Information Warfare AND South China Sea, Disinformation AND South China Sea, Misinformation AND South China Sea, Narrative Building AND South China Sea. The dataset contains 203 articles from well-known mainstream media and news from the LexisNexis website platform (Ali & Jatmiko, 2024). After being cleaned of duplication and contextual judgment, the data contained 136 articles and was saved in a .csv file for further preprocessing. Furthermore, data is transformed into a string and analyzed using pre-trained data processing using BART (Bidirectional and Auto-Regressive Transformer) -large-MNLI (Multi-Genre Natural Language Inference), a pre-trained model for news for Predicting Topics for News Articles (Isoaho et al., 2021). It is primarily used to determine the relationship between two pieces of text – typically a premise and a hypothesis – and classify that relationship into one of three categories: entailment (the hypothesis logically follows the premise), contradiction (the hypothesis contradicts the premise), and neutral (the hypothesis is neither entailed nor contradicted by the premise).

Meanwhile, the topic model using LDA (Latent Dirichlet Allocation) was utilized to analyze the text. Topic modelling was designed as a tool to organize, search, and understand vast quantities of textual information (Nayak et al., 2022). Despite all of the limitations on the data quantity due to niche-specific keywords, the pre-trained prediction topics and topic modelling have a proper, systematic and rigorous analysis in semantic structures.

Information Operation in the South China Sea Conflict

The emergence of the three warfares strategy, which focuses on public opinion shaping through the media, psychological, and legal warfare (Kania, 2016), also known as lawfare (Bueger & Edmunds, 2024), can be inferred as China's views on information as one of the critical aspects in gaining success in contemporary and next-generation warfare. This perspective was adopted following the US invasion of Iraq in 2003 (Harold et al., 2021), which then developed into the three warfares strategy and was implemented in every conflict in which China is involved. Furthermore, it provides the assumption that information operations and warfare are taking a significant part in China's global campaign, particularly in the SCS conflict. To support the implementation of the strategy, the development of a semantics strategy as part of the narrative and information operation has also been China's focus in recent years (Bhatt, 2024).

The deployment of information operations under the umbrella strategy of three warfares in the SCS is designed to wear out and undermine the will and capabilities of the adversaries, including the US and its allies, should an open conflict take place. Moreover, China is using its gray zone tactics to achieve its national and military objectives with a very limited deployment of conventional kinetic warfare capabilities (Lee, 2022). The strategy has significance as a force

multiplier for the kinetic strategy in military operations or non-kinetic strategy in political or diplomatic scenarios alike (Kania, 2016). Hence, media outlets have a significant role in augmenting the narrative developed within the three warfares strategy, particularly the media aspect, to shape the perceptions of regional and global audiences.

Similarly, the US and its allies view information operations in the SCS as a critical component of their strategy to counter China's assertive and unilateral actions. Several key perspectives on the counter strategy include the effort to achieve information dominance by countering Chinese disinformation and propaganda and the protection of critical information infrastructure to support information operations in the region (Hinck et al., 2021). Moreover, the US and its allies in the region, including the Philippines, Japan, and Australia, are working together to counter Chinese information operations by sharing intelligence, conducting joint military exercises, and coordinating diplomatic efforts (Garamone, 2023).

Both China and the US, along with their respective allies, recognize the importance of media in shaping public perception and influencing the strategic environment in the SCS. The use of media outlets and their publications can be used to extend and disseminate the political agenda and interest in the region. China uses state-controlled media outlets to disseminate narratives to support its claims and actions in the SCS, including promoting narratives that highlight China's historical ties and claims to the region while accentuating its supposedly peaceful intentions (Martin, 2021). Meanwhile, the US and its allies also leverage media outlets mainly to counter China's disinformation and propaganda campaigns by promoting transparency and the rule of law and disseminating accurate information about the current situation in the SCS (Hinck et al., 2021).

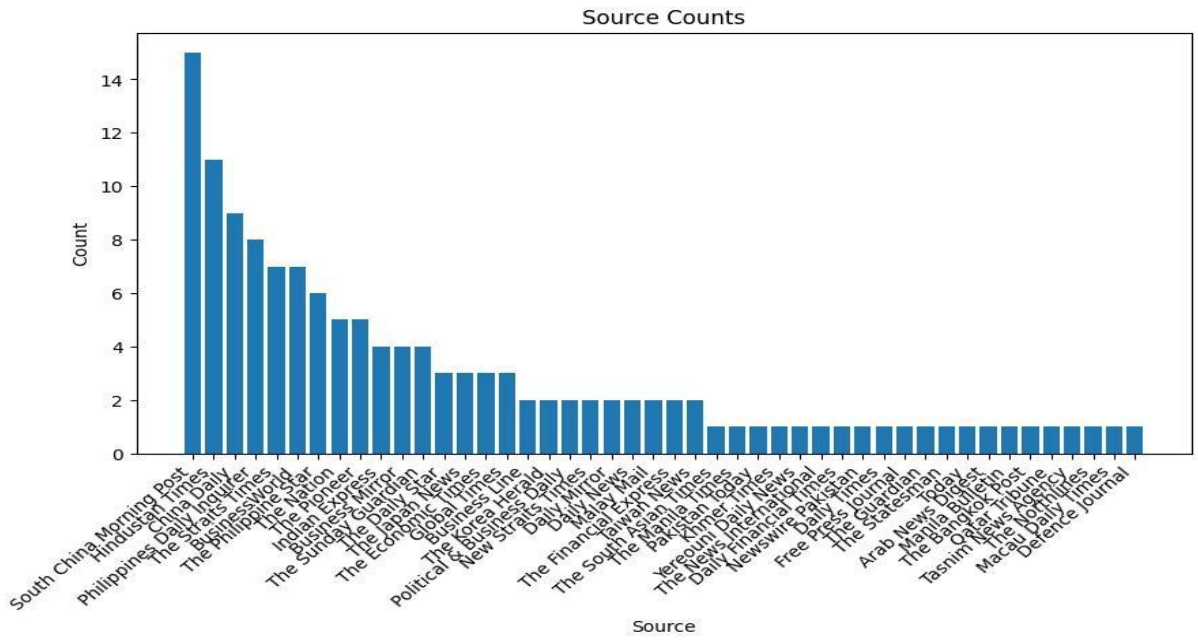
Based on the assumption that there is a positive correlation between news and media utilization with information operations purposes in the SCS conflict, this study analyzes the data collected to reveal the pattern of the utilization of media that supports the agenda of information operation regarding countries that take part in the conflict or have interest in the region.

Analysis Findings

Exploratory Data Analysis

Based on the EDA process, the depicted source of the mainstream media is shown in Figure 1 below, which shows the number of counts on the issue related to the SCS conflict in several mainstream media and news platforms. The number of news publications related to the issue in the SCS can be seen to correlate with the media platforms' affiliation with certain countries taking part in the regional conflict.

Figure 11.1: *The source counts of the mainstream media and news platforms.*



From this depiction, the researchers can trace the affiliation of the mainstream media to certain parties within the SCS conflict to infer the partiality of the platform in supporting certain agendas. Hence, the correlation between where the news publications are based and the use of certain narratives or information to support a specific agenda is pretty strong. This argument can be seen from the top news platforms that are affiliated with certain countries in the region, such as the *South China Morning Post*, *China Daily* to China, the *Philippines Daily Inquirer* to the Philippines, and *The Straits Times* and *Business World* to Singapore.

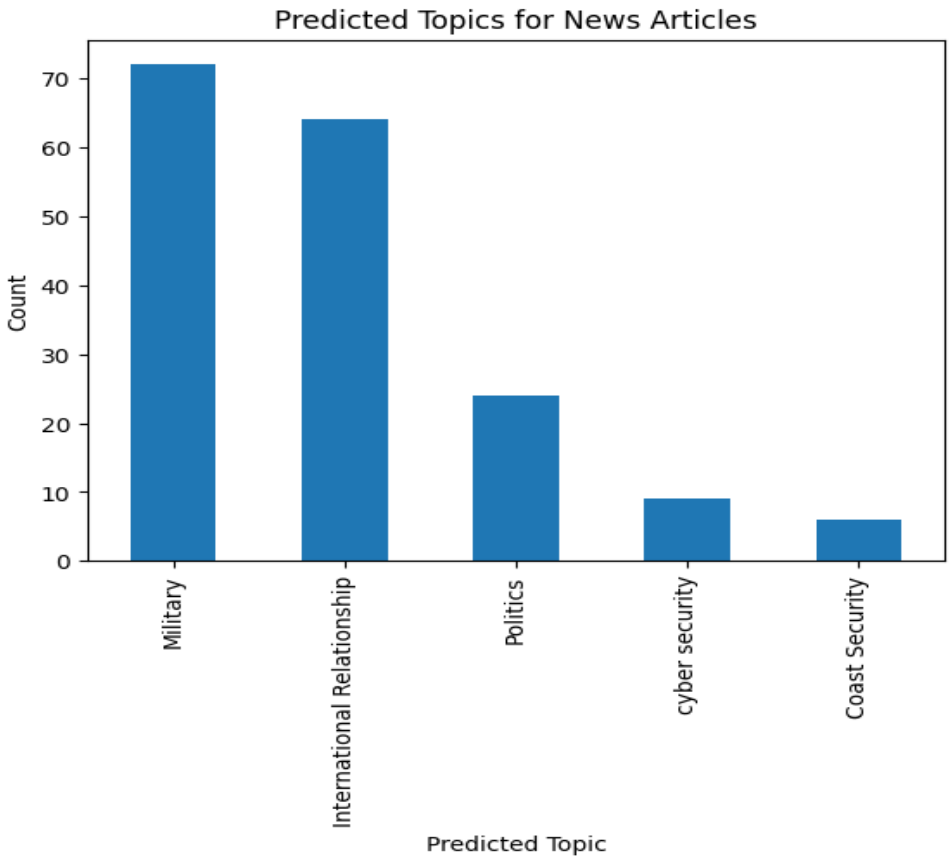
Interestingly, this study also finds that several media outlets not directly affiliated with the SCS claimant countries – such as the *Hindustan Times*, *The Pioneer*, and *Indian Express* – which are based in India, actively report on the issue, raising questions about their role and underlying affiliations toward the SCS' regional discourse. Furthermore, these findings spark curiosity about the agenda and interest of extra-regional countries, such as India, in the region. Further analysis of these findings may offer a more comprehensive understanding of the complexities of the information aspect, dwelling on the SCS issues.

Predicting topics for news articles

Based on the analysis method process, the bar chart shown in Figure 1 below shows the predicted topics for a set of news articles using the BART-large-MNLI model, as shown in Figure 2. Military is the most frequently predicted topic, with over 60 articles categorized under it. International relations are the second most common topic, with slightly fewer than 50 articles. Politics is the third most frequently predicted topic, with around 15 articles falling under this

category. Coast security is the least common, with fewer than 5 articles indicating specific security issues related to coastal areas. Cybersecurity is the second least common topic, with fewer than 5 articles.

Figure 11.2: *Predicted Topic of News Articles*



Focused analysis on less frequent topics could reveal emerging trends or overlooked issues. The BART-large-MNLI model's performance should be validated against a well-distributed sample of articles to ensure adequate coverage across all topics (Bhargava et al., 2021). This analysis provides a high-level overview of the topic distribution in the dataset as predicted by the BART-large-MNLI model.

Topic Modelling and Keyword Analysis

From the topic modelling analysis, this study found that the news being collected was heavily China-related news, particularly concerning its military and geopolitical actions. Military and strategic interests are significant themes across the dataset, and regional geopolitics are highlighted. Table 1 describes topics that seem relatively clear, given the terms provided.

Table 11.1: *Topic Modelling*

Topic	Terms
Topic 1	[‘force’, ‘warfare’, ‘space’, ‘strategic’, ‘operation’, ‘information’, ‘cyber’, ‘military’, ‘China’, ‘power’]
Topic 2	[‘China’, ‘India’, ‘say’, ‘Chinese’, ‘country’, ‘south’, ‘military’, ‘Philippines’, ‘Beijing’, ‘economic’]
Topic 3	[‘China’, ‘Pakistan’, ‘CPEC’, ‘India’, ‘Chinese’, ‘say’, ‘Indian’, ‘military’, ‘south’, ‘strategic’]
Topic 4	[‘China’, ‘say’, ‘military’, ‘Singapore’, ‘Chinese’, ‘defense’, ‘country’, ‘issue’, ‘national’]

Table 1 explains that Topic 1 revolves around military operations, strategy, information, and cyber warfare, with a particular focus on space and strategic power dynamics. The terms “cyber,” “military,” “space,” and “strategic” suggest discussions about modern military capabilities and strategic operations, possibly involving major powers like China and other major countries having keen interests in the SCS region. Topic 2 focuses on geopolitical relations in the Asia-Pacific region, specifically involving China, India, and the Philippines. The terms indicate discussions around military and economic power, as well as regional dynamics involving these countries, particularly related to the SCS issues. Topic 3 reveals an interesting finding with the appearance of words such as Pakistan and China-Pakistan Economic Corridor (CPEC), which seem to be out of the normal topic. Nevertheless, this topic may emerge due to the strategic implications and discussions around economic and strategic partnerships and rivalries in South Asia. Topic 4 seemingly revolves around the issue of China’s military in relation to the perspective of Singapore, which may consider the SCS issue as a major national issue in the country, particularly in the aspect of defense.

Furthermore, these topics and keywords extracted from the collected news articles and publications are depicted in Figure 3, which shows the cloud of the keywords from the dataset.

Figure 11. 3: *Cloud of keywords on the topic of information operation and warfare in the SCS based on the Countries mentioned.*

From the cloud in Figure 3, the algorithm manages to extract keywords with the word in a bigger size, signifying a greater number of mentions from the news articles. In contrast, the smaller keywords signify the small count of the particular keyword in the dataset. Unexpected findings that reveal words such as India and Pakistan as query findings, which are not directly related to the SCS issue, are assumed to have a deeper relation to the SCS issue or perhaps with China, particularly, which requires elaboration that may reveal an interesting new topic. However, this study takes precautions on such findings that are presumably irrelevant to the main discussed topics by ensuring that the appearance of the words is not merely a coincidence through several runs of topic modelling. The significance of the analysis results will highly depend on the interpretation and subject matter expertise on the related subject, particularly the topic that emerged and seemingly is out of the topic being discussed.

In topic modelling, the coherence score is a measure of how the topic is interpretable to the analysis or readers. The higher the score within the threshold means that the topic is easier to understand. Further, this analysis obtained a coherence score of 0.32 for the data analysis from the collected news might not be very high from the normal threshold for the score that goes between the scores of 0.3 to 0.7 on common coherence metrics are often considered good (Lim & Lauw, 2024). This score occurred because our keywords are niche and specific. Coherence score in topic modelling is a measure of the semantic consistency of topics. Mimno et al. (2011) emphasize the importance of coherence in topic modelling to determine topical consistency.

Figure 11. 4: *Percentage of the Topic Findings*

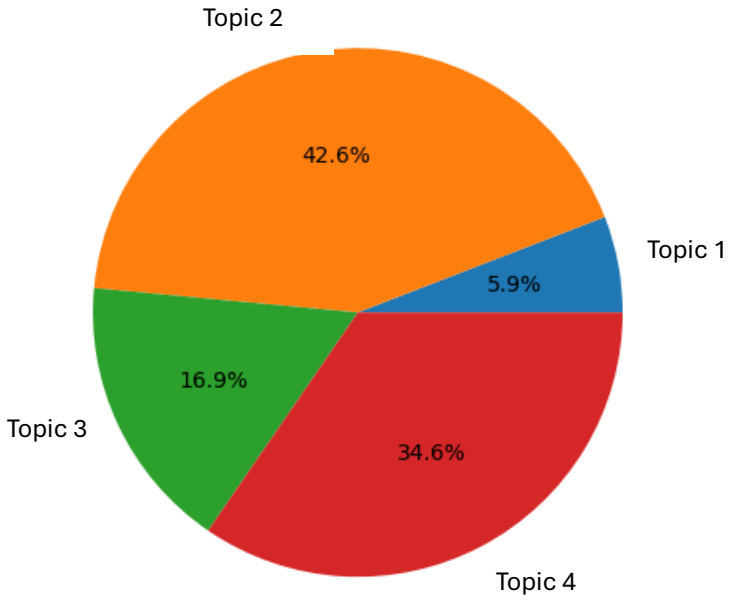


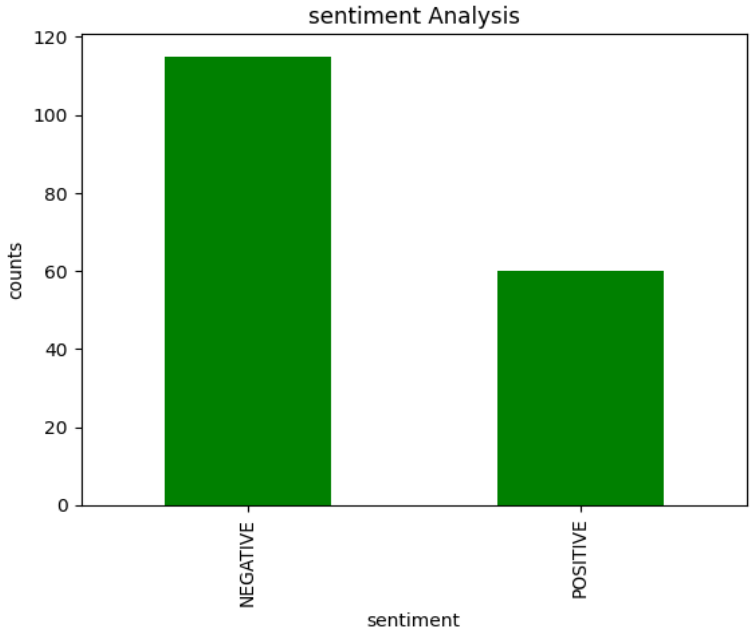
Figure 4 above describes the percentage of the issue findings of the SCS conflict. The issue was dominated by narration on military capabilities, strategic operations, and national and international policy stances. This study focuses on the two top issues as revealed in topic 2, revolving around geopolitical relations discourse on a strategic level that can be inferred to the SCS issue, and topic 4, discussing defense and military issues with the concentration on China and its surrounding countries, seemingly converging on the SCS region.

Sentiment Analysis

This research uses sentiment analysis to determine the emotional tone behind the news publications collected from the dataset to complement the other analysis methods and have meaningful insights. From the result of the sentiment analysis, this study gained insights into the sentiment contained in news publications. Figure 4 below depicts the result of the sentiment analysis conducted by this study.

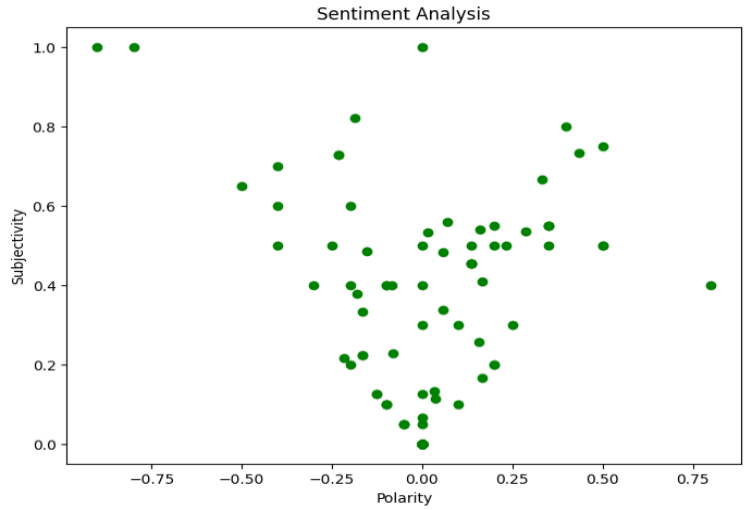
Through the performed sentiment analysis, several conclusions were derived regarding the tendency of the news publications regarding the issue of the SCS. Figure 5 presents a summary of sentiment assessments on the emotional tone where negative tones were obtained more frequently than positive tones, particularly the sentiment toward China.

Figure 11.5: *Sentiment Analysis Results on Tone*



Furthermore, Figure 6 shows the polarity and subjectivity of the language used in the news publication on the outlets and platforms.

Figure 11. 6: *Sentiment Analysis on Subjectivity and Polarity*



The figure describes polarity and subjectivity variables, which are used in the sentiment analysis to determine the overall language or opinion expressed in the text data. Polarity and subjectivity analysis have investigated many facets of sentiment categorization in textual data. Some studies concentrate on document-level polarity, while others advocate for entity-level analysis, such as organizations, particularly in financial subject articles that include many viewpoints (Rodrigues et al., 2015).

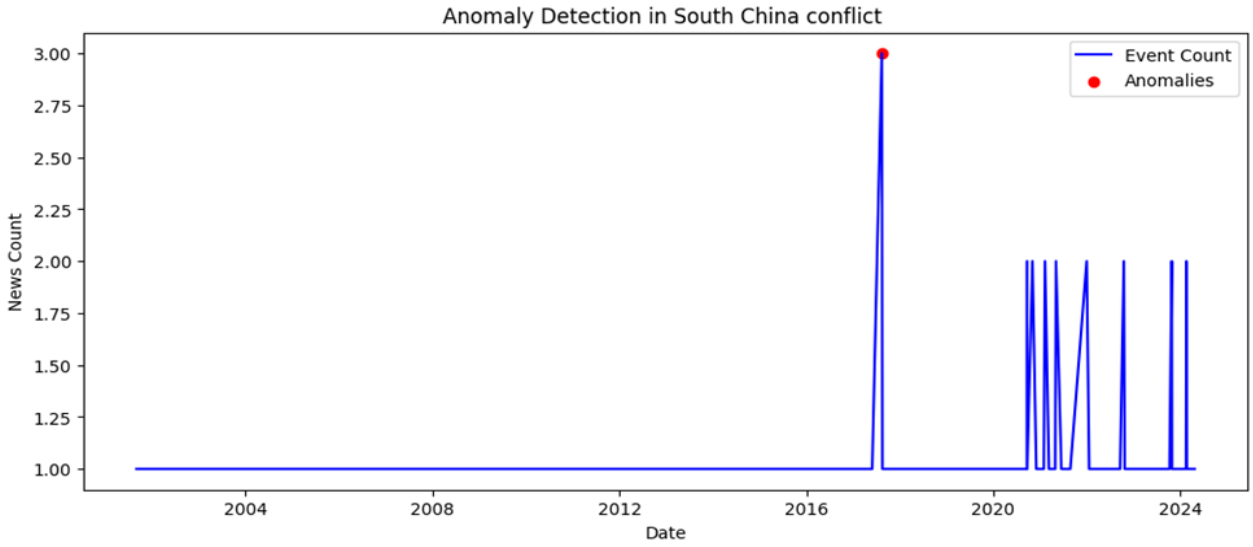
Polarity refers to the sentiment expressed in a piece of text, measured on a scale from -1 (most negative) to +1 (most positive). Negative polarity indicates negative sentiment, while positive polarity indicates positive sentiment. Neutral polarity (close to 0) means the sentiment is neither strongly positive nor negative (Satapathy et al., 2022). The analysis found that the average polarity score is around 0.16825, suggesting a slightly positive sentiment. Moreover, the minimum polarity found is -0.9, indicating some texts have a strong negative sentiment, while the maximum polarity found is 0.8, indicating the strongest positive sentiment in the data. The 25th and 50th percentiles are both approximately 0 (indicating a significant portion of the data has neutral sentiment), and 75% of the data has polarity values less than or equal to 0.8.

Meanwhile, subjectivity measures the degree to which a piece of text is more opinion-based (subjective) or fact-based (objective), ranging from 0 (completely objective) to 1 (completely subjective). Subjective text often contains personal opinions, emotions, or judgments, while objective text presents facts, figures, or statements with minimal personal bias. The average subjectivity is 0.165153, indicating that the majority of the text tends to be more objective than subjective.

Time Series Analysis

Time series analytics performed on the collected papers tries to reveal anomaly detection in media reports on the South China Sea conflicts that reveal significant fluctuations in coverage intensity over time, indicating key geopolitical developments. Time series analytics is one of the best analytics tools to reveal anomaly detection on a certain topic in media (Hellicar et al., 2016). The results of the time series analysis in the media are as follows:

Figure 11. 7: *Time Series Analysis on the South China Sea Issues*



The graphic above described from the early 2000s until 2016, media coverage of the South China Sea conflict remained at a stable baseline, with a consistent frequency of reporting. This suggests that, despite ongoing territorial disputes, the issue did not receive sustained international media attention. The relatively low and stable reporting trend during this period may reflect limited escalation in geopolitical tensions or a lack of major policy shifts from key stakeholders. A major anomaly in reporting intensity is observed in 2016, marking the most significant deviation from the established baseline. This sharp increase aligns with the 2016 South China Sea arbitration ruling by the Permanent Court of Arbitration (PCA), which invalidated China's claims under the Nine-Dash Line doctrine. The ruling, and China's subsequent rejection of it, led to heightened regional tensions, increased diplomatic discourse, and intensified military maneuvers, all of which likely contributed to the unprecedented surge in media coverage. The detection of this anomaly underscores the pivotal role of international legal decisions in instigating public debates and discourse over the already sensitive issue of territorial conflicts.

Following the 2016 anomaly, a shift in reporting dynamics is observed from 2019 onward, characterized by recurrent fluctuations in media coverage. Unlike the pre-2016 period, which exhibited a stable baseline, the post-2019 era shows irregular spikes in reporting frequency, indicating periodic escalations in regional tensions. These fluctuations may correspond to significant geopolitical developments such as increased military exercises, diplomatic confrontations, or policy shifts by key actors, including China, the United States, and ASEAN nations. The observed pattern suggests that the South China Sea conflict has transitioned into a more dynamic and frequently contested issue in global media discourse.

Trigram Analysis

Trigram analysis – a computational method identifying three-word phrases appearing with high frequency – provides further granularity into the recurring themes within the data collected for this paper. The trigrams analysis is able to capture frequent geopolitical phraseology as intended by this paper. Trigram analysis involves the analysis of three consecutive words and can be used to measure language similarity and clustering (Zamora et al., 1981). This technique helps uncover recurring strategic narratives, such as “South China Sea” (265 occurrences) and “People’s Liberation Army” (41 occurrences), which indicate dominant framing patterns in security discourse. The most frequently occurring trigrams are as follows:

Table 11.2: *Trigram Analysis Results*

Trigram	**Occurrences**
south china sea	265
west philippine sea	53
people liberation army	41
president xi jinping	26
east china sea	24
indo pacific region	21
line actual control	20
strategic support force	20
exclusive economic zone	19
liberation army pla	19

The trigram analysis provides insights into the key thematic elements of the dataset by identifying frequently occurring three-word phrases. These trigrams reveal significant geopolitical and military discourse, particularly related to China’s regional and global strategic positioning.

- South China Sea (265 occurrences) – This is the most frequently mentioned trigram, highlighting the prominence of the South China Sea as a critical geopolitical flashpoint. The region is central to territorial disputes involving China, the Philippines, Vietnam, and other neighbouring states, as well as strategic concerns for global powers such as the United States.

- West Philippine Sea (53 occurrences) – This term, used by the Philippines to refer to parts of the South China Sea within its exclusive economic zone, underscores the ongoing maritime disputes between China and the Philippines. The frequency of this trigram suggests significant discourse on sovereignty claims and regional tensions.
- People's Liberation Army (41 occurrences) – References to China's military, commonly known as the PLA, indicate a strong focus on China's defence strategies, military expansion, and regional security concerns. The presence of this trigram suggests discussions on China's military activities and its role in global geopolitics.
- President Xi Jinping (26 occurrences) – The inclusion of China's leader in the trigram analysis suggests discussions on his policies, leadership style, and strategic decisions regarding domestic and international affairs, including military and diplomatic initiatives.
- East China Sea (24 occurrences) – This trigram points to another major geopolitical hotspot, primarily involving territorial disputes between China and Japan. The frequency of this term highlights continued tensions over sovereignty claims in the region.
- Indo-Pacific Region (21 occurrences) – The presence of this trigram reflects discussions on broader regional security, particularly the strategic interests of the United States, Japan, Australia, and India in countering China's growing influence. This aligns with recent geopolitical trends emphasizing the Indo-Pacific as a critical theatre for global
- Line of Actual Control (20 occurrences) – This term refers to the contested border between China and India. The frequency of this trigram suggests that discussions on Sino-Indian territorial disputes, particularly in the Himalayas, remain relevant.
- Strategic Support Force (20 occurrences) – This phrase refers to a specialized branch of the PLA responsible for cyber, electronic, and space warfare. Its presence in the analysis suggests discourse on China's advanced military capabilities and the modernization of its defence strategies.
- Exclusive Economic Zone (19 occurrences) – This trigram pertains to maritime territorial rights and economic resource claims, particularly in disputed waters such as the South China Sea. Its frequency highlights ongoing legal and diplomatic disputes over maritime boundaries.

- Liberation Army PLA (19 occurrences) – This alternative phrasing for China's military reinforces the significant focus on defence and security matters, particularly in the context of China's strategic ambitions and regional military presence.

The trigram analysis reveals a strong focus on geopolitical and military themes, with particular emphasis on China's territorial disputes, military capabilities, and regional influence. The high frequency of terms related to the South China Sea, Indo-Pacific strategy, and the PLA indicates that these issues remain at the forefront of global security discussions. These findings align with broader geopolitical narratives, reflecting the strategic importance of maritime disputes, military modernization, and regional power dynamics.

Discussion

The findings from the EDA section on the source counts reveal the affiliation based on the country where the media outlets reside, which also aligns with the topic modelling in Table 1 and the cloud of keywords in Figure 3. Most of the news platforms reside in the countries that take part in the SCS conflict, or are located in the adjacent region, which makes their concern reasonable due to the proximity of their location to the center of gravity of the conflict. However, the findings of several media outlets located outside of the SCS region and its adjacent area, primarily from India, require further elaboration. Bhatt (2024) argues that India has interests in the SCS regarding its vital role in connecting India's trade route to countries in the Pacific. Any disruption to the shipping lanes would have significant economic consequences, particularly to India's national interest. Moreover, there are inherent interests of India in the region with India's joining the Quad (Quadrilateral Security Dialogue) strategic forum along with the US, Japan, and Australia, particularly India's will to counter China's growing influence in the Indo-Pacific region, starting from the SCS (Malhotra, 2023). These backgrounds provide motives for the appearance of several publications mentioning SCS issues in India-based news outlets.

In contrast, the findings of Pakistan in the topic modelling are actually mentioned due to its close relationship with China and its contrasting stance on the SCS issues that support China's agenda (Jamal, 2022). It is logical, considering the strong economic ties between Pakistan and China, with the China-Pakistan Economic Corridor (CPEC) as one of the keywords that emerged in the topic modelling. It can be inferred that the China-Pakistan relationship has raised concern in India that which has been included in the media discourse, hence shaping the public perception of the relationship.

The findings from the predicted topic for the news article in Figure 2 reveal an interesting thing about the nature of the conflict itself. It seems that military and international relationships are

the centre of the topics discussed. The use of the traditional approach in forwarding conventional military and security forces has become the predominant content in the information dissemination related to the conflict in the SCS. The result with the military topic as the highest confirms the assumption that the use of information in conflict complements the deployment of physical power assets, particularly as a force multiplier in influencing the behaviour of the other conflicting parties, and also shapes the global perception of the conflict itself, which is pretty much in play. With the consideration of the unacceptably high cost of an outright kinetic warfare or military clash, the potential of having an open conflict or outright war will be fairly low (Harold et al., 2021). Hence, a conflict that falls under the category of a gray zone would be the ideal option, particularly for China, with its primary objective to wear out its adversaries and to "win without fighting" by maneuvering beyond just simply operating in the gray zone, but further than that China has redefined and expanded the gray zone as the means to shape how other countries perceive the conflict (Lee, 2022). Therefore, the use of media outlets to spread disinformation as part of the three warfares becomes crucial.

On the topic of international relationships, it can be inferred that the concern about the conflict in the SCS will affect the stability and the relationship between countries in the region and probably extend to other regions with an embedded interest in the SCS. Meanwhile, the topic of politics, cyber security, and coastal security can be seen as the concern that follows the topic trends of military and international relations with more specificity.

From the sentiment analysis, we can see that the tendency of the news published regarding the SCS is leaning toward the negative emotional tone trend with China twice the amount of the positive tone. However, despite the negative tone, the language or text used in the news still has an average neutral sentiment that is signified by the average value of the polarity and subjectivity, which is close to 0. These contrasting results can be inferred to mean that the presentation of the news in the media platforms is inherently objective while conveying dismay or distrust toward the object of the news. In general, the expression of the news delivered in the media platforms mostly contains criticism of China's assertive strategy in the SCS issues (Sacks, 2022). Despite the media strategy contained in the three warfares, the negative sentiment holds the dominant trend toward China. This phenomenon takes place arguably due to the number of media platforms that are either based in countries with fair objectivity in perceiving the issue, such as Singapore, also a US ally, or in countries affiliated with China's adversaries, such as the US, the Philippines, and India.

From the time series analysis, it can be inferred that any anomaly in the data collection can be related to the phenomenon being analyzed, which in this paper is the South China Sea conflict. This anomaly pointed out a significant inflection point of the conflict that reached a certain height

of debates. The anomaly can signal the time allocation when a certain phenomenon takes place, then to take a deeper dive to analyze it closely. From the analysis, it seems that the inflection points of the conflict reach a new height after 2016. From that point, the anomaly seems to have a contraction, but not as high as before in 2016. However, it has still set a new stable line for the conflict to be considered a new global flashpoint.

Meanwhile, related to the time series analysis, the trigram analysis revealed that within the time allocation, the deeper granulation of the phenomenon being analyzed was with the three-word phrases that frequently appeared within the collected data. The numerous occurrences of certain trigrams show that in the data collected, these trigrams are overwhelmingly mentioned, which signify the volume of the discourse and also the spectrum of perception provided for the similar theme. Looking at the top three trigrams, the predominant discourse inclined to the South China Sea and the West Philippine Sea which refer to the same area from two different perspectives, the former is the most common name, while the latter is the narrative developed by the Philippines. Furthermore, the mention of the People Liberation Army (PLA) shows the dominance of the action taking place in the conflict area is related to the action conducted by the PLA or its affiliations. Nevertheless, both time series and trigrams analyses are agnostic without any inclination toward positive or negative sentiment in the results.

This study infers that the media are used by the respective parties for their potential in shaping the sentiment of the audience through the inclination of the narrative contained in the news and publications. The narratives are then influenced by the affiliation of the news platforms to the countries where they are based and the embedded national interests within the respective countries. Furthermore, this study assumes that the narratives published are correlated with the strategic level affiliations of the countries on certain issues discussed, such as the SCS issues. Nevertheless, the tools used in this paper could provide the analysis needed to investigate the narratives and sentiments used in the news to determine whether the news contributes to the benefit, or to the detriment, of the stakeholders involved in the conflict.

Contributions and Limitations

This study provides a broad depiction of media use in information operations in a conflict, taking the case of the SCS conflict. The findings reveal the strong correlation between mainstream media platforms, their utilization to narrate specific agendas, shaping the perception of the conflicting parties, and global audiences about certain issues taking place in the conflict. Some interesting revelations of the findings also contribute to a greater comprehension of the aspect of the conflict, such as the relations of the news media platforms outside of the region shaping the

perspective about the SCS issue. Moreover, this paper demonstrates the use of several useful tools to analyze data collection on a certain topic to determine the tendency of the news whether for the advantage or to the disadvantage of the stakeholders.

This study acknowledges several limitations that may influence the analysis. First, the restriction of LexisNexis, as the source of data collection, has on the counts of the news articles and platforms may limit the number of word queries assigned. Hence, the results from the methods may reveal excess findings that may not support the main topic of the study. Moreover, the limited word query included in the search keywords is deemed too general and could be refined for more specific results. Therefore, the findings are expected to be more generic. In addition, the study focuses on the media with English as the main language of communication. Hence, other mainstream media and news platforms that are not published in English are not included in the analysis. This exclusion may influence the findings of the result.

Conclusion and Future Research

The use of media outlets and platforms, regardless of the main media or alternatives, is increasing in its role in the dissemination of information or disinformation to support certain agendas related to the SCS conflict. Moreover, news outlets are increasingly seen as effective platforms for the dissemination of information by countries taking part in the SCS conflict to support the agenda in the conflict region and shape the perception of global audiences.

Regarding the issue of information operations in the SCS issue, seemingly, there is a battle of narratives taking place in the media between China and the US and its allies, trying to shape the international perception regarding the stance in the conflict. Regardless, information operations and warfare are only a part of the grand strategy launched by each side. While China has “three warfares” strategy, the US and its allies also build narratives and strategies to counter those strategies.

This study expects to initiate interest in the analysis of information operations and warfare in different strategic flashpoints and dimensions, which can contribute to the development of military studies. The extension of this study can be taken from the limitations mentioned in the previous section, which might be of interest to future research.

References

Ali, I., & Jatmiko, B. (2024). *LexisNexis Academic Dataset* [Exploratory data]. LexisNexis Academic.

Bhargava, P., Drozd, A., & Rogers, A. (2021). *Generalization in NLI: Ways (Not) To Go Beyond Simple Heuristics* (arXiv:2110.01518). arXiv. http://arxiv.org/abs/2110.01518

Bhatt, P. (2024). *Nine dash line: Deciphering the South China Sea conundrum*. Taylor & Francis.

Bueger, C. (2020). A Glue That Withstands Heat? The Promise. In E. R. Lucas (Ed.), *Maritime Security: Counter-terrorism lessons from maritime piracy and narcotics interdiction*. IOS Press.
Bueger, C., & Edmunds, T. (2024). *Understanding maritime security*. Oxford University Press.
Garamone, J. (2023, September 29). *U.S. official says allies acting together to deter China*. U.S. Department of Defense. https://www.defense.gov/News/News-Stories/Article/Article/3543179/us-official-says-allies-acting-together-to-deter-china/https%3A%2F%2Fwww.defense.gov%2FNews%2FNews-Stories%2FArticle%2FArticle%2F3543179%2Fus-official-says-allies-acting-together-to-deter-china%2F
Guan, K. C., & Koh, C. (2022). Maritime Security in Southeast Asia. In *Routledge Handbook of Maritime Security*. Routledge.
Harold, S., Beauchamp-Mustafaga, N., & Hornung, J. W. (2021). *Chinese disinformation efforts on social media*. RAND Corporation.
Hellicar, A. D., Rahman, A., & Koch, F. (2016, December). Time series analytics and collaborative agents research & design. *Time Series Analytics and Applications*.
Hinck, D. J., Ashburn, B., McNaughton, B., Heier, T., Liebold, T., & Pearce, R. (2021). A US Response to China's aggression in the South China Sea and overall aim of information dominance. *Journal of Indo-Pacific Affairs*, 362–378.
Isoaho, K., Gritsenko, D., & Mäkelä, E. (2021). Topic Modeling and Text Analysis for Qualitative Policy Research. *Policy Studies Journal*, *49*(1), 300–324. https://doi.org/10.1111/psj.12343
Jamal, U. (2022, February 7). *China and Pakistan Reiterate Support to Each Other's Core Interests*. https://thediplomat.com/2022/02/china-and-pakistan-reiterate-support-to-each-others-core-interests/
Kania, E. (2016, August 25). The PLA's Latest Strategic Thinking on the Three Warfares [Blog Post]. *CIMSEC*. https://cimsec.org/plas-latest-strategic-thinking-three-warfares/
Lee, D. J. (2022). Chinese information and influence warfare in Asia and the Pacific. *Hudson Institute*, 17.
Lehto, M., & Henselmann, G. (2020). *Proceedings of the 15th International Conference on Cyber Warfare and Security*.
Lim, J. P., & Lauw, H. W. (2024). Aligning Human and Computational Coherence Evaluations. *Computational Linguistics*, 1–60. https://doi.org/10.1162/coli_a_00518
Malhotra, A. (2023, May 1). India's relationship with the quad. *Georgetown Journal of International Affairs*. https://gjia.georgetown.edu/2023/05/01/engagement-not-entanglement-indias-relationship-with-the-quad/
Martin, M. (2021). China's Three Information Warfares. *U.S. Naval Institute Proceedings*, *147*(3). https://www.usni.org/magazines/proceedings/2021/march/chinas-three-information-warfares
Mimno, D., Wallach, H., Talley, E., Leenders, M., & McCallum, A. (2011). Optimizing Semantic Coherence in Topic Models. *Proceedings of the 2011 Conference on Empirical Methods in Natural Language Processing*, 262–272.
Nayak, P., Lakshmi, J. V. N., & Bhagat, V. V. (2022). Topic Modelling of ongoing conflict between Russia and Ukraine. *2022 International Conference on Trends in Quantum Computing and Emerging Business Technologies (TQCEBT)*, 1–8. https://doi.org/10.1109/TQCEBT54229.2022.10041450
Rodrigues, J., Cristo, M., Ferreira, J. Z., Fernandes, D., & Carvalho, A. (2015). Multi-Entity Polarity Analysis and Detection of Subjectivity in Financial Documents. *Journal of Information and Data Management*, *6*(2), Article 2. https://doi.org/10.5753/jidm.2015.1564
Sacks, B. J. (2022). *The Political Geography of the South China Sea Disputes: A RAND Research Primer*. RAND Corporation. https://doi.org/10.7249/PEA2021-1

Satapathy, R., Pardeshi, S. R., & Cambria, E. (2022). Polarity and Subjectivity Detection with Multitask Learning and BERT Embedding. *Future Internet*, *14*(7). https://www.mdpi.com/1999-5903/14/7/191

Teo, C. H. (2008). The acme of skill: Nonkinetic warfare. *Air and Command Staff College*, *30*, 43.

Wankhade, M., Rao, A. C. S., & Kulkarni, C. (2022). A survey on sentiment analysis methods, applications, and challenges. *Artificial Intelligence Review*, *55*(7), 5731–5780. https://doi.org/10.1007/s10462-022-10144-1

Zamora, E. M., Pollock, J. J., & Zamora, A. (1981). The use of trigram analysis for spelling error detection. *Information Processing & Management*, *17*(6), 305–316.

Chapter 12: Building EU defense capabilities for energy-tech hybrid warfare from Russia and China

Maurizio **Geri**, ORCID: https://orcid.org/0009-0009-8083-5211

Abstract:

Defense capabilities are assets and enabling capacities not only for the kinetic engagement but also for the non-kinetic part of the so-called ‘hybrid warfare’, 'grey zone/subthreshold' actions, or ‘destabilization campaigns’. The EU recently decided that it needs a stronger and more resilient defence industrial base and more ready and effective defense capabilities. This chapter discusses how to build better defense capabilities at the European level in order to deter, defend, and respond to the Russian and Chinese attacks in new realms of hybrid warfare, in particular the resources, energy and technology warfare.

Keywords: Energy Security, Hybrid Warfare, Destabilization

Introduction

This chapter focuses on how to better build European capability to deter and defend from so called ‘hybrid attacks’ from Russia, in particular in the energy sector, and from China in the resources and technology sector. After a short excursus on the hybrid warfare in energy and tech done by Russia and China towards Europe, the chapter introduces the EU’s new process of building common defense capabilities with the project Re-Arm Europe and concludes with recommendations on how to improve the EU defense capability cooperation for energy and tech security.

While Russia and China are adapting to rapid advances in modern military technology, the EU has lagged behind both in civilian and military tech, as the Draghi report on EU competitiveness in 2024 explained clearly (EU Commission, 2024b). The European defense industry is highly developed, producing top-tier weapon systems, however, it faces constraints in scaling up production. It struggles to keep pace with US contractors, who benefit from larger and more stable procurement budgets, as well as with emerging innovative start-ups in dual use technology. To tackle these challenges, European countries have begun to increase their defense spending, with expenditures of over €326 billion in 2024, rising 30% just in the previous 4 years, and investments of €102 billion, representing 30% of total defence expenditure (European Council, 2024a).

The EU has been working on the path of integrating its security and defence policies for decades, thinking about a common defense force and a defense industrial base already since 2017 with the European Defence Fund. But after the recent full-scale invasion of Ukraine and

Trump's second term, and in response to the international situation, the EU scaled up its goal to consolidate a common industrial base and launched the 'ReArm Europe' with a possible total budget of the 27 countries up to €800 billion (EU Commission, 2025c). The EU White Paper for European Defense Readiness 2030 stated that rebuilding European defence requires, as a starting point, a massive investment over a sustained period and provides a framework for the ReArm Europe plan (European Commission, 2025d). The White Paper also includes some elements of hybrid warfare, like protection of energy infrastructure or from cyberattacks. But it still lacks a coherent strategy and clear defense capabilities in this realm, in particular for energy and tech hybrid warfare. Furthermore, at the NATO 2025 Summit in the Hague, Allies pledged 5% of GDP annually in defense investment, of which 1.5% to, among other things, "protect critical infrastructures, defend networks, ensure civil preparedness and resilience, unleash innovation, and strengthen defence industrial base". Nevertheless, all this will require time, not only until 2030 but far beyond.

Hybrid warfare in energy and tech from Russia and China to Europe

As Russia tries to undermine support for Ukraine, besides divide the EU on its rearming phase, it is evolving its hybrid warfare tactics, which involve a combination of economic war, infrastructures sabotage (Parkes, 2025), cyber operations, disinformation campaigns and influence operations (Rensbergen, 2025). Russia started already in 2022 to manipulate gas flows (BBC, 2022), and more recently launched cyberattacks on critical infrastructure (Clark, 2024), and sabotaged undersea energy cables important for oil and gas platforms in the Baltic Sea (Braw, 2025), to keep Europe weak and ultimately reliant for energy on Moscow.

China is also escalating its use of hybrid warfare tactics in energy and technology areas against Europe (KCS Group Asia, 2025), including economic pressure and unethical practices like bribery, combined with reinforcing substantial dependencies of Europe in Chinese supply chain and value chain in Critical Raw Materials [CRMs] and technology necessary for the green energy transition (Maremonti, 2024). All these dependencies will be increasingly used by Russia and China as a tool of competition and hybrid warfare against Europe, which is why the EU has started decoupling and de-risking strategies from Russia and China (Lipke et al., 2024).

NATO and the EU are trying to adapt quickly to these new forms of hybrid war. NATO, since 2022 with the Strategic Concept of the Madrid Summit, warned of increased Russian and Chinese use of hybrid threats, even to the point of potentially leading to Art. 5 (Bajarunas, 2025). Today NATO is in the process to revise its hybrid warfare defense strategy after 10 years (Vohra, 2024; NATO, 2024), and the revised strategy will be presented in the next summit in June 2025 in

The Hague. The EU is also updating its hybrid warfare defense strategy (EU Commission, 2024b), including creating rapid response teams (EU Council, 2024). For both, one problem that remains is the 'hybrid warfare' catch-phrase, as it risks giving national countries responsibility to respond, limiting a rapid and effective European strategy against these tactics. A better definition would be 'transnational subversive' or even 'terrorist' activities by Russia (Latvian Institute of International Affairs, 2025), which is why NATO SECGEN talked recently about 'destabilization campaigns' (NATO, 2025a).

The main problem is that hybrid defense also requires a common defense capability that is still to be created and is not yet in the making especially at EU level. The EU, for example, considers as main pillars for the response to hybrid warfare: enhancing situational awareness; boosting resilience; providing an adequate response; recovery in case of crisis; and cooperating with organisations, such as NATO. But the EU does not have the means yet to put in practice these ways to reach its objectives. The EU new actions for example to enhance security of submarine cables (EU Commission, 2025b), are based on mapping of existing and planned Critical Undersea Infrastructures like pipelines and cables, a risk assessment and a security toolbox of mitigating measures. Nevertheless, the EU has not a force to be deployed immediately, or a defense capability to put in place to deter and defend from such attacks. One example of reaction by NATO, that the EU could follow, is the new 'Baltic Sentry' (NATO, 2025b), that is an increased military presence in the Baltic to guarantee critical infrastructure security.

Before seeing the EU cooperation in tech and energy security strengthened through building joint defensive capabilities, here are some critical aspects to take into consideration on the hybrid attacks.

The first issue to deal with is the **energy dependencies and vulnerabilities** of the EU. As said, Russia leveraged its energy resources as a weapon, exerting economic and political pressure through supply dependencies in Europe; and China is in process of doing the same, with Chinese investments in global energy infrastructure, through the Belt and Road Initiative, enhancing its influence over energy supplies also in EU partner countries around the world.

The second issue is about **rising cyber-attacks** facilitated by the increased digitalization of energy and technology infrastructures. Russian state-sponsored hackers have targeted EU countries with cyber-attacks aimed at critical infrastructure, both public and private (Orange Cyber Defence, 2024). Chinese cyber espionage aims to steal sensitive information and intellectual property from defense contractors or government agencies in EU, focusing on technological and military capabilities.

The third issue is to deal with technological innovation and competition in these sectors, in particular from China, as they are strongly investing in technologies needed for energy transitions, from batteries to chips, as well as in new emerging tech such as AI and quantum computing, to achieve superiority in technological capabilities, which can affect military readiness and response mechanisms in the EU. The EU is investing €200B Euro in AI innovation (EU Commission, 2025a), but this is still little compared to China.

Finally, it is important to increase military presence and exercises in these areas. Russia conducts military exercises near EU borders, showing their capabilities and signalling potential threats to the energy sector. Similarly, China is expanding its military presence in the South China Sea but also engaging in joint exercises with Russia. Therefore, Europe needs to raise its training and exercise in these sectors, showing the protection of energy and technology assets.

To conclude, to counter these hybrid threats the EU will need to enhance its hybrid warfare defense, developing strategies to counter the "weaponization of everything", and creating a common defense capability sooner than later. The crucial steps would be the definition of a hybrid warfare strategy, meaning ends, ways and means (Geri, 2025), to adapt both NATO and the EU with roadmaps for the necessary reforms (Genini, 2025), and then to build military means for a common defense capability against these types of warfare, to deter, defend and counter attack effectively in any moment. Next subchapter gives some recommendations for building specifically these defense capabilities.

EU Defense capabilities, funds and strategies

Before analysing the capability developments and the technological innovation processes in the field of security and defence for the EU, we need to mention that the continent has been improving its security and defence, but the momentum to really start to build common defence capabilities didn't arrive until the new century. Fifty years after the first EU process of defense integration (with the birth of the first military alliance in Europe, the Western European Union in 1954) the EU created the European Defence Agency [EDA] in 2004, to promote and facilitate defence integration between members states with three main important functions: supporting the development of defence capabilities and military cooperation among member states; stimulating defence Research and Technology [R&T] and strengthening the European defence industry; and finally acting as a military interface to EU policies (EDA, 2015). In 2007 the EDA adopted a strategy for European Defence, Technological and Industrial Base [EDTIB] (EDA, 2005), with a European

Defence Research & Technology [EDRT] strategy, as an adequate defense industrial base was not considered anymore to be sustainable on a national basis.

In 2024, the Ministers of Defence adopted as strategic guidance for EDA the 'Long-Term Review', which outlines five core tasks: identifying shared needs and priorities to ensure that Member States' armed forces have the capabilities they actually require; enabling collaborative defence research and innovation, to prepare the future of EU defence; harmonising requirements and engaging in joint capability development; aggregating demand towards joint procurement to fill capabilities shortfalls; and finally interfacing with EU civilian and defence policies (EDA, 2024a). All important elements but after guidance we need an application of that guidance, which needs to decide and apply 'ways and means' to reach those goals. In 2017 the EU therefore launched a European Defence Fund [EDF]] (EU Defence Industry and Space, 2024), for the industrial side of defence, in which until then member states were independent, that in the context of the multiannual financial framework for 2021-2027 has a small budget of € 8 billion, to finance multinational defence projects and stimulate defence industry cooperation. But again, this new program was still little for the defence of half a billion citizens in the 21st century, which was guaranteed for decades by NATO, the Transatlantic Alliance.

After the Russian war against Ukraine, things started to really change for the EU, and with the second Trump administration all the process started to accelerate. In October 2022 some NATO countries, scared by their lack of real defense from a possible Russian attack, created the European Sky Shield Initiative, launched by Germany, with the support of UK, Norway, Finland, Baltic states and other states in Central/Southeast Europe, to which Turkey, Poland and Sweden joined in 2024 (Duman, 2024). Furthermore, in September 2023 the EU Parliament adopted the Commission proposal on the European Defence Industry Reinforcement through common Procurement Act [EDIRPA], an instrument of just €500 million, to incentivise members to procure defence products jointly. At the beginning of 2024 the EU released the European Defense Industrial Strategy [EDIS], which aims to strengthen the EDTIB, suggesting to switch to a 'war economy war', and the European Defence Industry Program [EDIP] to strengthen EU defense capabilities with €1.5B from EU budget for 2025-2027 (Borrell, 2024) (asking to spend 50% of procurement in EU by 2030, and to collaboratively buy 40% of defence equipment by 2030) (EU Commission, 2024a). But it was only in March 2025, after Trump threatened to abandon Ukraine support, that the EU Commission President launched the "**ReArm Europe Plan**" (EU Commission, 2025c), to help EU countries to rearm quicker. Specifically, the Plan has three goals:

1) to activate the national escape clause of the Stability and Growth Pact, allowing members to increase significantly their defence expenditures without the 'Excessive Deficit Procedure';
2) to provide €150B of loans to members for defence investment, specifically for air and missile defence, artillery systems, missiles and ammunition, drones and anti-drone systems etc;
3) to use the EU budget, to direct more funds towards defence-related investments.

This plan seems big, but it says that it could unlock up to €800B of defense spending in the next few years, all depending on members ability to invest. Furthermore, as some scholars argue (Fiott, 2025), a risk today is that the injection of money could reinforce market fragmentation.

After this plan, the *White Paper for European Defense Readiness 2030* was published, to provide a framework for the ReArm Europe Plan and to outline a new defence strategy through a number of additional key actions, identifying also investment needs to close critical capability gaps and build a strong defence industrial base. The paper clarified that all initiatives aim at strengthening national armed forces, improving their interoperability in line with NATO standards, not creating a European army, as "member states will always be responsible for their armed forces" (EU Commission, 2025c). Then, it confirmed a new dedicated instrument for Security Action for Europe [SAFE] based on €150 billion loans on the capital markets based on funding approach to help member states increase investments, and identified seven priority areas: air and missile defence; artillery systems; ammunition and missiles; drones and anti-drones systems; military mobility; AI, quantum, cyber, electronic warfare; strategic enablers/infrastructure protection (EU Commission, 2025c).

Regarding the growing hybrid threats, including cyber-attacks, sabotage, electronic interference in global navigation and satellite systems, disinformation campaigns and political and industrial espionage. Specifically on how to deter and defend from possible weaponization of energy infrastructure, resources and the new technologies, and how to build strong defense capabilities in these sectors, the paper presents as said two priority areas: Artificial Intelligence [AI], Quantum, Cyber & Electronic Warfare (*defence applications using military AI and quantum computing and EU-wide advanced electronic systems*) where there is a need to develop together offensive cyber capabilities as credible deterrence; and the critical infrastructure protection, with strategic airlift and air-to-air refuelling aircraft, intelligence and surveillance, maritime domain awareness, use and protection of space etc. Apart from this there is not much on energy and technology wars protection though. So, let's see how to improve EU tech and energy security through common defense capabilities for these specific sectors.

Recommendations

As a premises, it's important to say that **developing and procuring capabilities through multinational cooperation** helps not only collective security but also to generate economies of scale, reduces costs, and give tech development and resilience through the spin-offs and satellite activities, which in turn help the general integration of a continent of half a billion people like the EU. Which is why it is urgent for the EU to start building defense capabilities together, as the ReArm Europe proposes, not only for kinetic and conventional warfare but also hybrid one as explained in this chapter. The problem is that the process will take long time, as European countries depend on the US for several "enablers", like the architecture for long-range detection, identification and tracking/geolocating of targets and for transmitting in real time the targeting data beyond line of sight, airborne electronic warfare, multiple types of munitions and military platforms, etc. Therefore, ReArm Europe is a good start, but deterrence and defence are not made by **budgets or industrial bases**, they are done by operational capabilities, good strategic planning and strategic enablers. Transforming the budget into capabilities is a long and complex process, so nobody knows exactly how many hundreds of billions the EU nations must spend, but mostly nobody knows how long it will take for much-needed defence common capabilities (Pugnet, 2024). Furthermore, EU countries will also have to start recruiting high-quality military personnel and train them with exercises that take time. First of all, the EU must create a strategy, to build common defense capabilities against hybrid warfare in tech and energy.

As in every **strategy**, first of all we need to define clear 'ends, ways and means'. The EU needs to have **clear goals** and clear objectives in these areas, like deter and defend from any external attack on European energy and technology security; improve EU resilience meaning withstand and recover from any attacks in these sectors; and finally to protect EU interests in these areas all around the world. To do that the EU needs joint production and procurement of military capacities and joint actions to defend in these realms of hybrid warfare.

Also, regarding the relationship with NATO, the EU should have as clear goals, to establish its capabilities in relation to NATO, as the 'European pillar of NATO', meaning in a complementary not substituting way. In particular, it should enhance its 'Strategic Autonomy', meaning develop independent military and strategic capabilities so the EU can address crises without over-relying on NATO or the U.S., while still cooperating closely; deepen its coordinated defense planning, aligning defense planning and capabilities development among EU member states to avoid duplication and ensure interoperability with NATO forces; and finally supporting a common EU

Defense Policy to strengthen the EU's own crisis management and military operations framework, to complement NATO's efforts.

Regarding **ways**, here are some ideas on where the EU should focus besides building a common industrial and technology base:

- *Development of Resilient Energy Infrastructure:* EU can work on reinforcing the energy infrastructure of member states. This includes investing in renewable energy sources, diversifying energy supplies, and enhancing the resilience of the grid against attacks.
- *Technological Innovation and Research:* Promoting research and development in emerging technologies such as artificial intelligence, blockchain, and advanced monitoring systems will help the EU stay ahead of hybrid threats.
- *Joint Exercises and Training:* Conducting joint military exercises that emphasize hybrid warfare scenarios can prepare EU forces to respond effectively. This includes training on cyber defense, disinformation campaigns, and the protection of critical energy infrastructure.
- *Enhanced Intelligence Sharing:* Improving intelligence sharing mechanisms among member states can lead to better situational awareness and quicker response times. Establishing a secure, centralized database for hybrid threats could enhance cooperation.
- *Investment in Cybersecurity and digital protection:* strengthening cybersecurity defense, including a digital shield and investing in most advanced technologies to counter cyber threats (Edwards, 2025).
- Giving priority to investment in dual use technology with the objective of defragmenting defence markets and gradually integrating value chains and supply chain in tech and energy.

Furthermore, the **EU should follow NATO experience and best practices**, as NATO is more advanced with respect to the EU in common defense and collective security. For example, the EU should have a 'Defence Planning Process', which is an important step to identify and prioritise the capabilities required for military operations. The EU should also work more closely with private industry, similar to what NATO is doing with its new DIANA project, to foster industrial and technological cooperation, promoting also private finance of European defense (Riley et al., 2025). Another NATO lesson learned for the EU is how to improve its interoperability process with common rules of engagement in order to make the defense in this sector efficient. For the EU to enhance common defense capabilities means also to reduce tech and defense regulations, that

limit the possibility to build common capabilities, and to adapt at speed and scale to new military and defense tech.

Also, the EU should develop a common 'Command and control' [C2] as a respectable force must be employable. Currently there is no C2 at EU level. Therefore, the EU should create it, as until now the EU is under the NATO C2 (Council of the EU, 2019). That would require careful integration of existing institutions, clear delegation of authority, and consensus among member states. In particular as a legal basis it would require amending existing treaties (e.g., Treaty on European Union); creating a 'Central Command Authority', a civilian-military organization responsible for strategic planning and operational command; each member state appointing military and civilian representatives to this 'European Defense Command'; establish clear procedures, for operational decisions, possibly using qualified majority voting to balance sovereignty and efficiency; and a political leadership by the European Council for guidance and oversight.

Finally, regarding **means,** EU member states spent €326 billion on defense in 2024, more than double that of Russia. But they are divided as they don't spend time together. So, first the EU must increase common defence expenses together to have a competitive defense industry. To ensure that the EU has the necessary resources, innovation, and cooperation to meet security challenges in these areas it needs to reform the European Defence, Technological and Industrial Base [EDTIB] mentioned earlier. In particular EDTIB needs to improve:

- *Coherent member capacities*: EU's EDTIB includes a variety of defense companies, ranging from large multinational corporations to **small and medium-sized enterprises** [SMEs], each contributing to various domains. But big companies and small companies do not have the same ability to scale up so there needs to be a harmonization of tools at EDTIB level.
- *Collaborative procurement:* the EU countries should collaborate to buy European defense technology, leveraging collective buying power to acquire advanced systems more efficiently.
- *Innovation and research:* EU encourages research and development in next-generation technologies through initiatives like the EU Innovation Fund, which invests in start-ups and innovative projects that can enhance military capabilities, but it is still a small fund.
- *Standardization and interoperability*: improve efforts to standardize equipment and systems across member countries to enhance interoperability during joint

operations. This involves adhering to EU standards and guidelines, so much remains to be done.

- *Emerging Technologies:* Increase focus on cybersecurity capabilities and the integration of emerging technologies, such as AI, big data analytics, and advanced communication systems.
- *Supply Chain Resilience:* work more in common to ensure resilience in the defense industrial base, reducing dependency on any single source or external supplier. To address potential stockpile shortages because of the support to Ukraine, the EU needs also to understand the industrial perspective on its production capacity and supply chain vulnerabilities, particularly in the areas of munitions, critical technologies and strategic minerals

Finally, the other tools mentioned earlier that the EU needs to expand are also the European Defence Industry Reinforcement through common Procurement Act [EDIRPA], that as said has now only €500 million, to incentivise members to procure defence products jointly and the European Defence Industry Program [EDIP] to strengthen EU defense capabilities, that now has €1.5B from EU budget for 2025-2027 (Borrell, 2024). Finally, the EU annual budget, that usually is around €200 billion, has for security and defense operations only 1%. This cannot be sustainable nowadays so there has to be a great shift also on this point, even taking into account that the risk of national criticism moving funds from social and economic support to defense, could fuel stronger nationalist right-wing movements that could even destroy the European projects.

As Latin said, mala tempora currunt, bad times are upon us. But by focusing on these goals, ways and means, the EU can build a robust strategy and defense posture against the growing challenges posed by kinetic war and also hybrid war from Russia, China and others in future.

Acknowledgements

Maurizio Geri's research is funded by the European Union MSCA (GA number 101105349)

Disclaimer

Views and opinions expressed are those of the author(s) only and do not necessarily reflect those of the European Union or Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

References

Bajarunas, E. (2025, February 11). Using NATO's Article 5 against hybrid attacks. *CEPA*. https://cepa.org/article/using-natos-article-5-against-hybrid-attacks/

BBC. (2022, September 29). Nord Stream 1: How Russia is cutting gas supplies to Europe. *BBC*. https://www.bbc.com/news/world-europe-60131520

Borrell, J. (2024). Time to strengthen European defence industry. *EEAS*. https://www.eeas.europa.eu/eeas/time-strengthen-european-defence-industry_en

Braw, E. (2025, January 3). Russia's cable-cutting could threaten Europe's whole energy supply. *Foreign Policy*. https://foreignpolicy.com/2025/01/03/russia-baltic-sea-cable-cutting-incidents-gas-oil-energy-norway/

Clark, S. (2024, November 22). Winter is coming. So are Russia's elite hackers. *Politico*. https://www.politico.eu/article/russia-hackers-europe-winter-energy-infrastructure-moscow-gas-hike-digital/

Council of the EU. (2019, April 23). The EU Concept for Military Command and Control. https://data.consilium.europa.eu/doc/document/ST-8798-2019-INIT/en/pdf

European Defence Agency. (2005, January 1). *Background.* https://web.archive.org/web/20070613071057/http://www.eda.europa.eu/genericitem.aspx?area=Background&id=122

European Defence Agency. (2015). *Mission and functions.* https://eda.europa.eu/who-we-are/Missionandfunctions

EDA. (2024a, May 28). EU Defence Ministers approve reinforced mandate for EDA. https://eda.europa.eu/news-and-events/news/2024/05/28/eu-defence-ministers-approve-reinforced-mandate-for-eda

EDA. (2024b). The European Defence Fund at a glance. https://defence-industry-space.ec.europa.eu/eu-defence-industry/european-defence-fund-edf-official-webpage-european-commission_en

EU Commission. (2025a, February 11). EU launches InvestAI initiative to mobilise €200 billion of investment in artificial intelligence. *Press Corner*. https://digital-strategy.ec.europa.eu/en/news/eu-launches-investai-initiative-mobilise-eu200-billion-investment-artificial-intelligence

EU Commission. (2025b, February 21). Commission and the High Representative present strong actions to enhance security of submarine cables. *Press Corner*. https://ec.europa.eu/commission/presscorner/detail/en/ip_25_580

EU Commission. (2024a, March 5). First ever defence industrial strategy and a new defence industry programme to enhance Europe's readiness and security. *Press Corner*. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1321

EU Commission. (2025c, March 19). Commission unveils the White Paper for European Defence and the ReArm Europe Plan/Readiness 2030. *Press Corner*. https://ec.europa.eu/commission/presscorner/detail/en/ip_25_793

EU Commission. (2025d, March 19). Joint White Paper for European Defence Readiness 2030. https://ec.europa.eu/commission/presscorner/api/files/document/print/sl/qanda_25_794/QANDA_25_794_EN.pdf

EU Commission. (2025e, March 19). Questions and answers on the Defence Package: White Paper for European Defence - Readiness 2030. *Press Corner*. https://ec.europa.eu/commission/presscorner/detail/pl/qanda_25_794

EU Commission. (2024b, September 9). The future of European competitiveness: Report by Mario Draghi. https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en#paragraph_47059

EU Commission. (2024c, December 11). Commission proposes measures to strengthen border security and counter hybrid threats. *Directorate-General for Communication*.

https://commission.europa.eu/news/commission-proposes-measures-strengthen-border-security-and-counter-hybrid-threats-2024-12-11_en

European Council. (2024a). *EU defence in numbers.* https://www.consilium.europa.eu/en/policies/defence-numbers/

EU Council. (2024b, May 22). Commission welcomes the Council approval of the Guiding framework for the practical establishment of the Hybrid Rapid Response Teams. *Press Release*. https://www.consilium.europa.eu/en/press/press-releases/2024/05/21/hybrid-threats-council-paves-the-way-for-deploying-hybrid-rapid-response-teams/

EU Defence Industry and Space. (2024). The European Defence Fund at a glance. https://defence-industry-space.ec.europa.eu/eu-defence-industry/european-defence-fund-edf-official-webpage-european-commission_en

Fiott, D. (2025, March 5). Spending our way out of a crisis? The challenges and benefits of rearming Europe. *CSDS, VUB*. https://csds.vub.be/publication/spending-our-way-out-of-a-crisis-the-challenges-and-benefits-of-rearming-europe/

Genini, D. (2025, February 25). Countering hybrid threats: How NATO must adapt (again) after the war in Ukraine. *New Perspectives, Online First*.

Geri, M. Ends, Ways, and Means. NATO and the EU need closer cooperation to counter a hybrid war, especially against the energy sector. *GMF Insights*. https://www.gmfus.org/news/ends-ways-and-means

KCS Group Asia. (2025, January 7). Hybrid warfare – the coordinated efforts of Russia and China against the West. https://kcsgroup.com/hybrid-warfare-the-coordinated-efforts-of-russia-and-china-against-the-west/

Latvian Institute of International Affairs. (2025, February 10). “Hybrid war” thinking hobbles Europe’s response to Russian sabotage. https://liia.lv/en/opinions/hybrid-war-thinking-hobbles-europes-response-to-russian-sabotage-1367

Lipke, A., Oertel, J., & O’Sullivan, D. (2024). Trust and trade-offs: How to manage Europe’s green technology dependence on China. *European Council on Foreign Relations*. https://ecfr.eu/publication/trust-and-trade-offs-how-to-manage-europes-green-technology-dependence-on-china/

Maremonti, F. (2024, August). EU’s technological dependencies towards China: The case of EV batteries. *Reconnect China, Policy Brief*, 13. https://www.reconnect-china.ugent.be/wp-content/uploads/2024/09/Reconnect-China_Policy-Brief-13_EUs-Technical-Dependencies-towards-China.pdf

NATO. (2024, May 7). Countering hybrid threats. https://www.nato.int/cps/ru/natohq/topics_156338.htm?selectedLocale=en

NATO. (2025a, January 15). Opening remarks by the Chair of the NATO Military Committee, Admiral Rob Bauer and NATO Secretary General Mark Rutte at the meeting of the Military Committee in Chiefs of Defence. https://www.nato.int/cps/en/natohq/opinions_232160.htm?selectedLocale=en

NATO. (2025b, January 14). NATO launches 'Baltic Sentry' to increase critical infrastructure security. https://www.nato.int/cps/en/natohq/news_232122.htm

Orange Cyber Defense. (2024, December 5). Security Navigator 2025 reveals Europe as top target for hacktivism, with groups shifting focus to cognitive warfare. *Press Release*. https://newsroom.orange.com/securitynavigator/

Pugnet, A. (2024, September 26). Unknown price of EU defence reform sets up budget battles. *EURACTIV*. https://www.euractiv.com/section/defence/news/unknown-price-of-eu-defence-reform-sets-up-budget-battles/

Roderick Parkes, R. (2025, 7). Sabotage as signal: Why attacks on maritime infrastructure challenge our model of sense-making. *CSDS Policy Brief*. https://csds.vub.be/publication/sabotage-as-signal-why-attacks-on-maritime-infrastructure-challenge-our-model-of-sense-making/

Roussi, A., Braun, E., Griera, M., & Pollet, M. (2024). Huawei bribery scandal rocks European Parliament. *Politico*. https://www.politico.eu/article/belgian-police-raid-huawei-lobbyists-as-new-scandal-rocks-eu-parliament/

Riley, A., Taylor, P., & Davis, S. (2025, March 11). How to promote private finance of European defence: Two views. *European Policy Center*. https://epc.eu/en/Publications/How-to-promote-private-finance-of-European-defence-Two-views~62d8b0

Van Rensbergen, A. (2025, January 21). Hybrid threats: Russia's shadow war escalates across Europe. *The Parliament*. https://www.theparliamentmagazine.eu/news/article/hybrid-threats-russias-shadow-war-escalates-across-europe

Vohra, A. (2024, May 12). NATO to revise strategy on how to tackle hybrid warfare. *Deutsche Welle*. https://www.dw.com/en/nato-to-revise-strategy-on-how-to-tackle-hybrid-warfare/a-70959822

Chapter 13: Wargaming Tomorrow's Threats: Fostering Critical Thinking Through Simulation-Based Learning

Tali Neumann, CMO at Wikistrat

Abstract:

This paper examines the application of red teaming methodologies and Structured Analytic Techniques (SATs) as pedagogical tools for developing critical thinking skills. Drawing from Wikistrat's extensive experience implementing simulation-based learning environments, the paper presents case studies that demonstrate how these methodologies challenge cognitive biases, encourage multidimensional analysis, and prepare students for complex decision-making environments. As technological and social factors increasingly impede critical thinking development, structured methodologies provide an essential framework for educators seeking to cultivate these vital skills in their students.

Keywords: Wikistrat, Red-Teaming, Simulation-Based Learning, Wargaming

Introduction

In an era of unprecedented information accessibility and algorithmic curation, the development of critical thinking skills has never been more crucial or more challenging. Critical thinking—the ability to analyze, evaluate, and synthesize information objectively—serves as the foundation for informed decision-making across disciplines, from academic research to military strategy and corporate leadership. Despite universal acknowledgment of its importance, educational institutions worldwide struggle to effectively cultivate these skills in their students.

A study by Cambridge University Press (2019) polling 1,000 teachers globally revealed concerning statistics: 85% of teachers felt their students lacked sufficient critical thinking skills upon entering university, 50% struggled to find time to develop effective teaching methods for these skills, and only 21% believed they had adequate materials to develop students' critical thinking capabilities. These findings highlight a significant gap between recognizing the importance of critical thinking and successfully implementing pedagogical strategies to foster it. This paper explores how red teaming methodologies, as implemented through Wikistrat's simulation-based approaches, provide effective frameworks for developing critical thinking skills.

The Critical Thinking Crisis: Barriers and Challenges

Technological Impediments to Critical Thinking

The digital landscape presents significant challenges to critical thinking development. Social media algorithms create what Babis (2020) describes as "echo chambers," where users predominantly encounter viewpoints that align with their existing beliefs, reinforcing rather than challenging their perspectives. This algorithmic curation significantly reduces exposure to diverse viewpoints—a prerequisite for developing robust critical thinking skills.

Media consumption patterns further exacerbate this problem. News outlets increasingly rely on emotionally-charged, attention-grabbing headlines designed to maximize engagement rather than inform. NBC News (2013) notes that users frequently share articles based solely on headlines without reading the full content, bypassing critical evaluation of the information presented.

The emergence of generative AI tools like ChatGPT represents another potential obstacle. Unlike traditional search engines that provide multiple sources for evaluation, these tools deliver seemingly authoritative answers without transparent citation of sources. As IE University (2023) observes, this can lead to reduced information evaluation and critical interpretation by users, who may accept AI-generated content without questioning its accuracy or bias.

The Reboot Foundation (2021) characterizes these trends as a "steady erosion of critical thinking," leaving individuals vulnerable to manipulation and misinformation. As technological tools increasingly mediate our information consumption, the ability to think critically becomes not just an academic skill but a practical necessity for navigating daily life.

Cognitive Biases: The Inherent Obstacles

Even without technological factors, human cognition itself presents barriers to critical thinking through inherent biases that shape how we process information, as Azzopardi (2021) notes, emphasizing how biases can distort information retrieval. These biases include:

1. **Confirmation Bias**: The tendency to search for, interpret, and remember information that confirms existing beliefs while discounting contradictory evidence. This bias often manifests when analysts prematurely settle on a favored hypothesis and interpret subsequent information through that lens, as was evident in historical intelligence failures like the Bay of Pigs invasion. Thomas and Rielly (2017) explain that once a decision is made, individuals often overlook contradictory intelligence, reinforcing the approved plan despite evidence to the contrary.
2. **Groupthink**: The unconscious pressure to conform to the views and positions of one's social or professional group, often at the expense of critical evaluation. Group members often conform to early opinions, suppressing dissent—shown by

Sunstein & Hastie's (2014) jury studies where confident jurors abandoned their views to match others. This phenomenon becomes particularly dangerous in high-stakes decision-making environments, where team cohesion can inadvertently suppress dissenting viewpoints that might identify flaws in analysis.

3. **Failure of Imagination**: The tendency to dismiss unlikely scenarios without thorough consideration, limiting the range of possibilities examined. As the 9/11 Commission Report famously noted, this bias can lead analysts to discount low-probability, high- impact events simply because they seem implausible based on historical precedent.
4. **Availability Heuristic**: The inclination to focus on scenarios that are particularly salient or similar to recent events rather than systematically examining alternatives. As demonstrated by Cherry (2023), this creates systematic distortions in risk assessment— leading people to fear memorable but rare events while ignoring commonplace dangers.

These cognitive biases operate largely below conscious awareness, making them particularly difficult to identify and overcome without structured methodologies specifically designed to counter their effects. Friedman (2023) emphasizes that overcoming these biases necessitates the implementation of intentional strategies to reduce their impact on decision-making. Beyond analytical techniques, Wikistrat addresses these biases by deliberately assembling diverse crowds of experts for each simulation—from different geographical regions, professional backgrounds, and disciplines—a composition that helps counter confirmation bias, mitigates failure of imagination, and reduces the availability heuristic's influence through exposure to varied global perspectives. This approach aligns with Karadzhov et al. (2024), who demonstrated that cognitive diversity enhances group decision-making by mitigating biases.

Figure 13. 1: *A comparative table mapping key cognitive biases to specific Structured Analytic Techniques (SATs) that help counteract them, emphasizing the practical application of analytical tools.*

COGNITIVE BIASES AND STRUCTURED COUNTERMEASURES

COGNITIVE BIAS	DESCRIPTION	COUNTER-TECHNIQUES	APPLICATION
Confirmation Bias	Favoring information that supports existing beliefs	ACH, Devil's Advocacy	*Election Interference* Simulation
Groupthink	Conforming to group views and suppressing dissent	Team A / Team B	*Putin Goes Nuclear* Simulation
Failure of Imagination	Dismissing implausible yet high-impact scenarios	Pre-Mortem Analysis, Black Swan Backcasting	*Israel Strikes Iran, NYU Horizon Scanning*
Availability Heuristic	Overestimating the likelihood of memorable or recent events	Structured Scenario Development	*Global Risk Prediction* exercise

Red Teaming: A Structured Approach to Critical Thinking

Conceptual Framework

Red teaming provides a structured methodology for challenging assumptions and biases by deliberately taking adversarial or alternative perspectives. This approach involves assigning a group (the "Red Team") to question an organization's strategies, assumptions, and decisions by simulating the perspective of competitors, threats, or alternative viewpoints. The core strength of red teaming lies in its ability to institutionalize the practice of challenging assumptions and exploring blind spots. By creating a formal process and space for questioning conventional wisdom, red teaming overcomes the social and organizational pressures that often suppress critical perspectives. This methodology helps participants develop critical thinking skills by:

1. Forcing examination of problems from multiple perspectives
2. Requiring explicit questioning of assumptions
3. Exploring a broader range of possibilities than would naturally occur
4. Creating psychological safety for dissenting viewpoints

These features make red teaming particularly valuable as a pedagogical tool for developing critical thinking skills in educational settings, as highlighted by Tufts University (2024), underscoring its effectiveness in challenging assumptions and promoting deeper analysis.

Structured Analytic Techniques: Enhancing Critical Thinking

While red teaming provides an overarching methodological framework for challenging assumptions, Structured Analytic Techniques (SATs) offer specific analytical tools that enhance critical thinking more broadly. As Heuer and Pherson (2020) note, these techniques were developed within the intelligence community to mitigate cognitive biases and improve analytical rigor. When integrated into educational contexts, they provide students with concrete procedures for organizing information, exploring relationships, and evaluating hypotheses.

Key Structured Analytic Techniques

Alternative Competing Hypotheses (ACH)

The ACH technique requires analysts to identify all plausible hypotheses and systematically evaluate evidence against each one. Rather than looking for confirming evidence, ACH emphasizes disconfirmation—focusing on evidence that would refute a hypothesis. This approach directly counters confirmation bias by forcing consideration of alternative explanations. According to the US Government (2009), ACH is particularly valuable for controversial issues, as it helps develop a clear record of considered theories and reasoning behind judgments.

Devil's Advocacy and Team A/Team B Exercises

Devil's advocacy involves assigning individuals or teams to challenge prevailing views by arguing for alternative positions. This technique institutionalizes dissent, making it psychologically safer to question dominant perspectives. The Team A/Team B approach establishes separate analytical teams that examine the same problem from different starting assumptions, with Akhmad et al. (2021) showing that devil’s advocacy enhances decision quality by increasing the exploration of alternatives, especially in groups prone to closed-mindedness

Structured Scenario Development

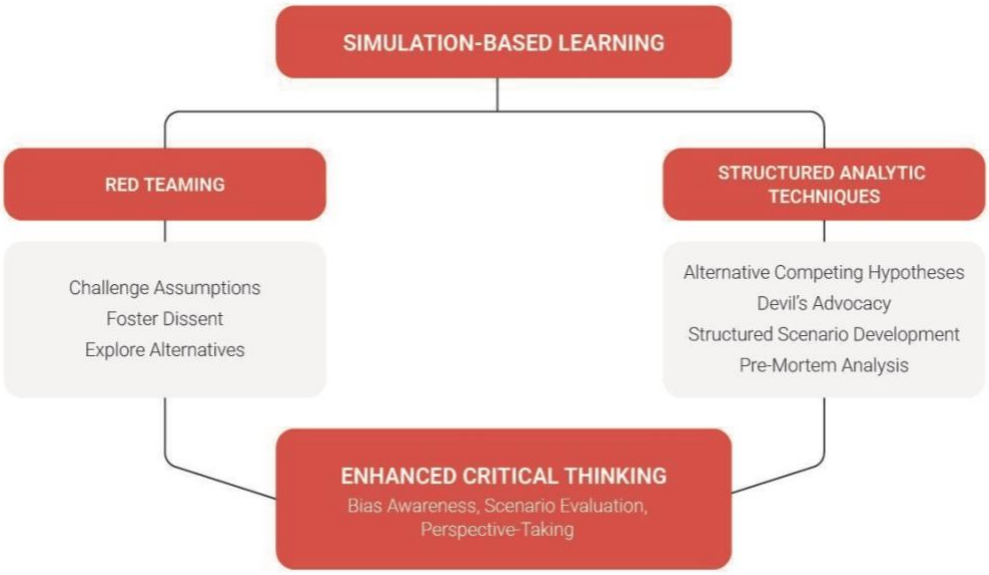
Structured scenario development techniques help analysts systematically explore the implications of different future conditions. These methods typically involve identifying key driving forces, critical uncertainties, and potential outcomes to construct plausible future scenarios. According to Cordova-Pozo and Rouwette (2023), this approach enhances strategic decision-making by incorporating future orientation, external context focus, and narrative plausibility.

Pre-Mortem Analysis

Pre-mortem analysis, developed by psychologist Gary Klein, asks participants to imagine that a plan or strategy has failed and then work backward to determine what could have caused the failure. It addresses the Failure of Imagination bias by compelling participants to actively envision and analyze potential failures—even scenarios considered improbable or previously overlooked. This structured method encourages participants to expand their mental frameworks and systematically explore risks they might normally ignore due to perceived implausibility. As Serrat (2017) explains, this technique fosters a more realistic and thorough planning process by anticipating potential pitfalls before they materialize.

Figure 13. 2: *A conceptual framework diagram illustrating how red teaming and SATs interact to foster critical thinking by encouraging adversarial analysis, structured exploration of alternatives, and systematic bias mitigation.*

Framework for Cultivating Critical Thinking via Red Teaming and SATs



Wikistrat's Implementation: Case Studies in Simulation-Based Learning

The following timeline illustrates the general structure followed in Wikistrat's simulation-based learning exercises, which typically unfold in sequential phases designed to maximize experiential learning and critical reflection.

Figure 13.3: *A timeline representing the sequential phases of Wikistrat's simulation-based learning process.*

Case Study 1: "Become Your Own Enemy" - Election Interference Simulation

This classic red teaming exercise involved participants role-playing potential adversaries attempting to interfere with U.S. elections. Participants were divided into teams representing Russia, China, and Iran, with each participant assigned the role of a decision-maker within these foreign entities. The simulation unfolded in three phases:

1. Participants researched their assigned actor's strategies and goals while experimenting with tools available for influence operations
2. Participants created sample materials that could be used in disinformation campaigns
3. Participants switched to roles as American decision-makers tasked with developing defensive strategies against the threats created in the first phase

This approach developed critical thinking by requiring participants to:

- Understand motivations and constraints of adversaries
- Consider vulnerabilities from an attacker's perspective
- Develop practical experience with the mechanisms of information warfare
- Evaluate defensive strategies against realistic threats

The simulation's effectiveness stemmed from its experiential nature—participants didn't simply discuss theoretical possibilities but actively engaged in developing and countering realistic threats.

Case Study 2: Stress-Testing Conventional Wisdom - "Putin Goes Nuclear"

This crisis management simulation challenged the conventional wisdom that Russian nuclear threats represent mere bluffing. The simulation utilized the devil's advocate methodology combined with wargaming to explore an unconventional scenario where Putin actually employs tactical nuclear weapons. Participants played teams representing Russia, Ukraine, and the United States. The simulation began with a nuclear threat by Putin that wasn't taken seriously, followed by a second phase where he actually deployed a nuclear weapon against a Ukrainian logistics hub for Western aid. This approach developed critical thinking by:

- Forcing participants to consider low-probability, high-impact scenarios
- Requiring analysis of how different actors would respond to unprecedented events
- Challenging status quo assumptions about nuclear deterrence
- Exploring cascading consequences across multiple domains (military, diplomatic, economic)

Case Study 3: Structured Scenario Development - "When Israel Strikes Iran"

This simulation employed structured scenario analysis to examine three potential outcomes of an Israeli strike on Iran's nuclear facilities:

1. A successful Israeli strike
2. A failed Israeli strike

3. A partially successful Israeli strike

For each scenario, participants analyzed how different actors (Iran, USA, China, Russia, and Saudi Arabia) would react, addressing key questions about the impact on Iran's nuclear strategy, regional involvement, relations with major powers, and domestic stability. This case study directly implemented structured scenario development techniques by methodically varying a key uncertainty (strike success) while systematically exploring implications across multiple domains. The approach incorporated Team A/Team B exercises as different groups analyzed the same geopolitical problem from the perspectives of various regional and global actors.

This structured approach fostered critical thinking by:

- Requiring systematic comparison of different outcomes
- Forcing consideration of second and third-order effects
- Analyzing how different actors with varying interests would respond to the same event
- Identifying key decision points and indicators that would signal which scenario was unfolding

Case Study 4: Backcasting Black Swans - "Risks to Global Stability"

The Backasting methodology counters the failure of imagination bias by deliberately analyzing unlikely scenarios with high potential impact, a central concept in strategic innovation and foresight, as emphasized by Fayet and Férey (2023). The approach involves identifying potential "black swan" events and then working backward to determine what factors could lead to them. This methodical approach transforms abstract possibilities into concrete risk factors that could be monitored and addressed through structured analysis. Wikistrat has been implementing this approach in annual horizon scanning simulations with NYU's Risk Prediction course, where students collaborate with Wikistrat experts to predict risks to global stability in the coming year. Beyond examining expected risk categories (political, geopolitical, social, economic), the simulation explicitly includes a category dedicated to shock events. This approach developed critical thinking by:

- Normalizing consideration of low-probability, high-impact events
- Creating a structured process for analyzing unlikely scenarios
- Requiring identification of early warning indicators
- Teaching students to distinguish between impossibility and improbability

Additionally, the collaboration between students from different institutions and experts, expands cognitive horizons: "[What I found most valuable was being exposed to] the different perspectives. It was great to read the ideas from students and professionals worldwide. It helped

me step outside myself and see things from a different point of view," reflects one NYU student. Another student notes: "looking at such a variety of thoughts and analyses was incredibly insightful and a fascinating project that left me feeling more knowledgeable (if worried…) about the world."

Case Study 5: Examining Success Scenarios - "Pearl Harbor from the Japanese Perspective"

This historical simulation challenged participants to consider not just failure scenarios but also the downstream consequences of successful actions. By examining this historical event from this untraditional perspective, participants gained insight into how "success" in one context might create new challenges in others. The simulation highlighted Admiral Isoroku Yamamoto's observation after Pearl Harbor: "I fear all we have done is to awaken a sleeping giant and fill him with a terrible resolve"—illustrating how tactical success can lead to strategic failure if broader consequences aren't considered. This approach developed critical thinking by:

- Challenging the assumption that success is an endpoint rather than a transition
- Requiring consideration of unintended consequences
- Examining how success in one domain might create vulnerabilities in others
- Encouraging systems thinking about complex international relationships

Conclusion

As we navigate an era characterized by information abundance yet increasing vulnerability to manipulation, these structured approaches to critical thinking development represent essential components of educational practice across disciplines.

The combination of red teaming methodologies with structured analytic techniques creates a comprehensive framework for developing critical thinking skills. Where red teaming provides the adversarial perspective necessary to challenge assumptions, SATs offer the analytical rigor required to systematically explore implications and evaluate alternatives. Together, they address multiple dimensions of critical thinking—from perspective-taking and assumption-questioning to systematic evaluation and metacognitive awareness. The methodologies demonstrated through Wikistrat's simulations offer valuable models for educators seeking to bridge the gap between recognizing the importance of critical thinking and successfully cultivating it in their students.

About Wikistrat

Wikistrat is the world's first crowdsourced consultancy, employing a distinctive collaborative model to produce unique insights and innovative solutions. Wikistrat leverages a global network of

leading experts—including former executives, academics, military leaders, and innovative thinkers—who collaborate on an interactive online simulation platform. This collaboration is further enhanced by Wikistrat's specialized gamification methodology, which structures interactions to maximize creativity, engagement, and insight generation.

References

Cambridge University Press. (2019, March 7). Critical thinking: Survey results. Cambridge University Press ELT. https://www.cambridge.org/elt/blog/2019/03/07/critical-thinking-survey-results/

Babis, D. (2018, July 30). Tearing down media echo chambers with AI. Good Audience. https://blog.goodaudience.com/tearing-down-media-echo-chambers-with-ai-c25363e68802

IE Insights. (2023, January 27). ChatGPT and the decline of critical thinking. IE University. https://www.ie.edu/insights/articles/chatgpt-and-the-decline-of-critical-thinking/

NBC News. (2013, January 28). TRMS headline writing challenge: 'Infoxication'. NBC News. https://www.nbcnews.com/news/world/trms-headline-writing-challenge-infoxication-flna1c8146661

Reboot Foundation. (2021, June). The state of critical thinking 2021. Reboot Foundation. https://reboot-foundation.org/the-state-of-critical-thinking-2021/

Friedman, H. H. (2023, July). *Cognitive biases and their influence on critical thinking and scientific reasoning: A practical guide for students and teachers. SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2958800

Azzopardi, L. (2021). Cognitive biases in search: A review and reflection of cognitive biases in information retrieval. *Proceedings of the 2021 Conference on Human Information Interaction and Retrieval (CHIIR '21)*, 27-37. https://doi.org/10.1145/3406522.3446023

Tufts University. (2024, December 12). *Building skills for better decision-making in crises.* The Fletcher School. https://fletcher.tufts.edu/news-events/news/building-skills-better-decision-making-crises

Fayet, H., & Férey, A. (2023, March 30). *Imagining beyond the imaginary: The use of red teaming and serious games in anticipation and foresight*. Security Studies Center. Ifri - Institut français des relations internationales. https://www.ifri.org/en/memos/imagining-beyond-imaginary-use-red-teaming-and-serious-games-anticipation-and-foresight

Thomas, T., & Rielly, R. J. (2017). What were you thinking? *Biases and rational decision making*. *InterAgency Journal*, 8(3), 98–105. https://thesimonscenter.org/wp-content/uploads/2017/08/IAJ-8-3-2017-pg98-105.pdf

Karadzhov, G., Vlachos, A., & Stafford, T. (2024, February 2). *The effect of diversity on group decision-making*. arXiv. https://arxiv.org/html/2402.01427v1

Heuer, R. J., & Pherson, R. H. (2020). Structured analytic techniques for intelligence analysis (3rd ed.). CQ Press.

Akhmad, M., Chang, S., & Deguchi, H. (2021). Closed-mindedness and insulation in groupthink: Their effects and the devil's advocacy as a preventive measure. Journal of Computational Social Science, 1-23. https://doi.org/10.1007/s42001-021-00061-6

Cordova-Pozo, K., & Rouwette, E. A. J. A. (2023). Types of scenario planning and their effectiveness: A review of reviews. Futures, 149, 103153. https://doi.org/10.1016/j.futures.2023.103153

US Government. (2009). A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis. Central Intelligence Agency. Retrieved from https://www.cia.gov/resources/csi/static/Tradecraft-Primer-apr09.pdf

Serrat, O. (2017). The premortem technique. In Knowledge solutions (pp. 311–314). Springer. https://doi.org/10.1007/978-981-10-0983-9_22
Sunstein, C. R., & Hastie, R. (2014). Making dumb groups smarter. Harvard Business Review, 92(12), 90-98. https://hbr.org/2014/12/making-dumb-groups-smarter
National Commission on Terrorist Attacks Upon the United States. (2004). The 9/11 Commission Report: Final report of the National Commission on Terrorist Attacks Upon the United States. U.S. Government Printing Office. https://9-11commission.gov/report/
Cherry, K. (2023, September 5). *What is the availability heuristic? How this mental shortcut affects decisions and leads to bias*. Verywell Mind. https://www.verywellmind.com/availability-heuristic-2794824

Glossary

ACH (Alternative Competing Hypotheses)

A structured analytic technique that requires analysts to identify all plausible explanations for an issue and evaluate evidence against each one, rather than in favor. This counters confirmation bias by promoting disconfirmation-based analysis.

Backcasting

A foresight tool where analysts start from a hypothetical future (often a black swan event) and reason backward to identify the chain of events that could lead there. Used to uncover hidden risks and early warning indicators.

Black Swan Events

Unpredictable, rare, and high-impact events that are often dismissed due to their perceived implausibility. Preparing for such events encourages imagination and long-range strategic thinking.

Cognitive Biases

Systematic errors in thinking that affect judgments and decision-making.

Devil's Advocacy

An SAT that assigns a person or group to argue against a prevailing idea or policy, regardless of personal belief. It challenges group consensus and surfaces potential weaknesses in reasoning or strategy.

Pre-Mortem Analysis

A forward-looking method where analysts assume a strategy has failed and then work backward to determine what could have caused the failure. It helps mitigate failure of imagination and surfaces overlooked risks.

Red Teaming

A methodology that assigns individuals or groups to play the role of adversaries or challengers in order to stress-test assumptions, expose vulnerabilities, and foster critical thinking. It institutionalizes dissent and encourages exploration of alternative perspectives.

Simulation-Based Learning

An experiential education technique where participants engage in realistic, interactive scenarios to practice decision-making and develop critical thinking.

Structured Analytic Techniques [SATs]

A set of formalized methods used to mitigate cognitive bias, improve analytical rigor, and enhance judgment. Common SATs include ACH, pre-mortems, devil's advocacy, and scenario development.

Structured Scenario Development

An SAT used to build and assess multiple plausible future situations by identifying key driving forces, critical uncertainties, and potential outcomes. It encourages strategic foresight and systems thinking.

Team A/Team B Exercise

A structured debate format where two teams analyze the same issue from different assumptions or perspectives. This technique highlights bias, promotes diverse thinking, and reduces groupthink.

Wargaming

A simulation exercise that models conflict or strategic scenarios, often involving role-play, to evaluate options and anticipate outcomes. Frequently used in military, academic, and corporate strategy settings.

Chapter 14: Geopolitical Futures and Force Structure Planning

Robert **Addinall**
Ali **Dizboni,** ORCID: https://orcid.org/0000-0002-8979-3953
Peter **Gizewski**

Abstract:
The use of strategic foresight has served as an important tool in military concept and capability development and military planning in an uncertain world. Exemplary is the use of foresight in the Canadian Army Land Warfare Centre's Future Army Project – a study examining the development of four alternative futures and their implications for Army concept and capability development circa 2040. Scenarios developed aimed at encouraging examination of future possibilities as opposed to prediction. That said one such scenario – entitled Global Quagmire exhibits characteristics akin to those at work in today's international security environment. Re-examination of the scenario in light of ongoing trends and drivers in the international system nevertheless highlights significant differences in the forces driving the system toward a Quagmire world. In particular, the development and use of information technologies has served to generate ideational and material impacts not entirely foreseen in the scenario's initial formulation. The result may be characterized as a "High-Tech" Quagmire in which various material and ideational forces interact with the use of communications technology and AI to stoke societal polarization and political extremism, environmental and economic decline and the increased pursuit of state security and survival through short term, reactive and often zero-sum strategies and policies.

Keywords: Futures and Foresight, Geostrategy/Geostrategic, International Security Environment, Ideational drivers, Material drivers, small and medium powers, Revisionist powers, Defence Policy, NATO

Introduction

The central arguments of this chapter are that the events and trends of recent years point towards a global security environment that can be characterized as a high tech quagmire, which can be defined as: A world in which various material and ideational forces combine (interact) with the use of communications technology and AI to stoke societal polarization and political extremism, environmental and economic decline and the increased pursuit of state security and survival through short term, reactive and often zero-sum strategies and policies. This type of emerging world carries with it the implication that larger, full spectrum armed forces will be needed, as playing niche roles while relying on larger allies may no longer be a viable strategy. This has the further implication that small and medium countries, as well as those with larger economies that have had

the latitude to spend a small percentage of their GDP on defence, will have to make changes in economic structure and political culture to enable evolution in this direction.

This position is substantiated through the following analysis. First, an outline of the Canadian Future Army Process conducted approximately a decade ago, culminating in three guidance publications between 2015 and 2017, is provided. This includes a brief overview of the foresight methodology used and the four future world scenarios that were generated and examined. Second, a brief assessment of how drivers and trends from 2017 to 2025 compare to those outlined up to 2017 is made. It is worth noting that events post 2017 reflect one of the future scenarios more than the other three – but a reassessment of all four is needed. Third, the variations for force structure implications in each scenario are considered. Given this three part analysis, it is argued that full spectrum forces that incorporate rapidly emerging technologies are most likely needed. This returns to the core thesis: full spectrum forces are a more expensive type of force structure to build and maintain, meaning that pressure on small and medium sized countries, including the majority of NATO countries, to spend two percent or more of GDP on defence is likely to continue unless trends change significantly.

The Canadian Future Army Process

A model using four future worlds set at a 2040 time horizon were developed using a strategic foresight and futures process that included five contributing methodologies. The first of these was environmental scanning, which was described in the Canadian Army reports as:

> …a process involving the acquisition and use of information about events, trends and relationships that may have a strategic bearing on how an organization does business… it also involves the use of four basic techniques (*undirected viewing, conditioned viewing, and informal and formal search of primary and/or secondary sources of information*) (Canadian Army Land Warfare Centre, 2015, p. 20).

Second was a Futures Wheel, described as: “comparable to what is more commonly referred to as structured brainstorming and… aligned closely with mind mapping… [which] allows a representation of complex interrelationships between trends” (Canadian Army Land Warfare Centre, 2015, p. 20). A third methodology involved the use of hindsight and learning from the past, with the explanation that:

> ...past experience often filters and conditions the impact of evolving trends and drivers on states, societies and the organizations and individuals that make them up. To this end, historical analysis of trends, drivers and their potential impacts is also employed to help ensure that observations and conclusions advanced are adequately informed by an

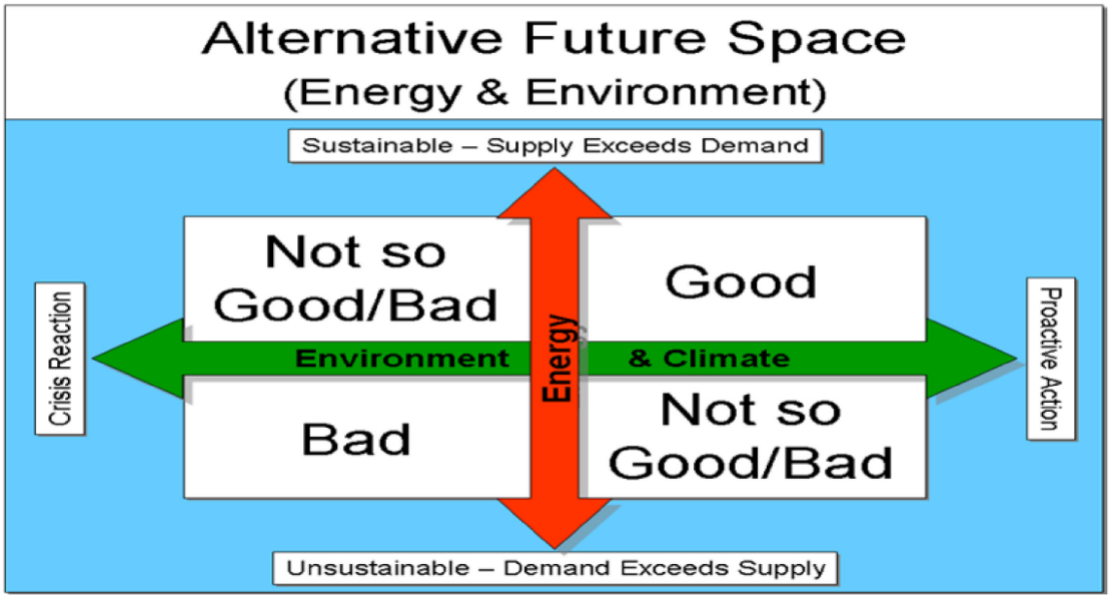
appreciation of past history and context (Canadian Army Land Warfare Centre, 2015, p. 22).

Unlike environmental scanning and future wheels that refer to current events and future linkages, this method is deeply informed by history. The fourth methodology used was Red Teaming, described as the selection of one member of the core futures team to monitor and participate in group discussions with the aim to question the team's fundamental assumptions, lines of reasoning employed in advancing arguments and conclusions (Canadian Army Land Warfare Centre, 2015, p. 22). This method helps check the negative effects of groupthink.

A seminar war game cycle aimed at examining the force implications of each of the four worlds followed. Each seminar war game included a wide range of both military and civilian participants from a variety of fields. The majority of participants were Canadians, but some Americans and participants from other NATO countries were also involved. The result was the above-mentioned three publications issued in 2015 to 2017: *Canada's Future Army, Volume 1: Methodology, Perspectives and Approaches*, *Canada's Future Army, Volume 2: Force Employment Implications*, and *Canada's Future Army, Volume 3: Alternate Worlds and Implications*.

To generate the future world scenarios key drivers emerging from the process were plotted onto impact-uncertainty axes with two drivers assessed as having the highest level of uncertainty and the greatest potential impact: energy sustainability and global environmental change. See figure 1:

Figure 14. 1: *Impact Uncertainty Axes and Alternative Futures*



Source: (Gizewski, 2017, p. 3)

The quadrants defined by the two axes in Figure 1 provided the basis for the four worlds. The upper left Not so Good/Bad quadrant formed the basis for the Materialism Gone Mad world. This was seen as a future in which energy supply exceeds demand (*that is, energy supply is sustainable*), but in which the globe continues to take a reactive stance on the environment. It reflects a world which would be abundant in energy, but one in which states show little regard for the natural environment (Gizewski, 2017, p. 3). The upper right Good quadrant defined what was called the High Octane 'Green' World. This was seen as a future in which global energy supply would exceed demand, and, at the same time, in which the world would be taking a proactive approach to the environment. It was anticipated to be characterized by a plentiful and sustainable energy supply and the development of an increasingly proactive stance towards the environment within societies and among states, including through proactive conservation as opposed to mere efforts aimed at environmental clean-up (Gizewski, 2017, pp. 3-4). The lower left Bad quadrant was defined as Global Quagmire. This was described as a future in which energy supply would be increasingly scarce or unsustainable, and in which the globe would have a reactive approach to the environment. In the Global Quagmire, states and societies would confront a dwindling energy supply yet take a highly reactive approach to the environment. The world would be experiencing an energy crisis along with growing international competition for the resources that would be left (Gizewski, 2017, p. 4). The lower right Not so Good/Bad quadrant provided the basis for the Recyclable Society world – a future in which energy would be scarce, with demand exceeding supply, but also one in which global actors would be taking proactive approaches to the environment. Its key characteristics were anticipated to be widespread energy scarcity and a proactive stance on the environment in which, as with High Octane 'Green' World, proactive conservation takes place instead of merely attempts to clean-up the environment (Gizewski, 2017, pp. 4-5).

Across all four scenarios there was a general assumption that uncertainty would represent a predominant characteristic of the future security environment. For that reason, accurate prediction would be impossible (Canadian Army Land Warfare Centre, 2015, p. 17). Future world scenarios were not expected to be perfectly accurate predictions but rather benchmarks which can be revisited at regular intervals in order to identify major trends and patterns in unfolding events.

Given geopolitical events between 2017 and 2025, the Global Quagmire world is of particular interest. A number of its characteristics resemble recent developments, including a failure to effectively implement solutions to deal with environmental issues, a zero-sum view of international affairs in many parts of the world, and pessimistic, short-term and reactive views of security and how it is achieved.

Current Trends and Drivers

The most notable departure from the Global Quagmire scenario as formulated around 2015-2017 is that, as of 2024, no true resource scarcities have yet arisen, although there are some caveats to this point. From the point of view of managing climate change the sustainability of ongoing fossil fuel production and use is questionable. In addition, the potential for scarcities to arise in key resources such as lithium for battery production exists. Furthermore, concerns over potential adversaries controlling most of the supply of certain key materials for both military and civilian production such as copper, gold, graphite and cobalt already led the United States to attempt to expand production of these resources in friendly countries under the Biden administration (e.g., CBC, 2024). The first months of the second Trump administration starting in early 2025 are suggestive of a potentially more uncertain, high impact, zero-sum thinking turn in this pattern, with the White House repeatedly making aggressive statements indicating an American interest in annexing Greenland and Canada, and also pressuring Ukraine into agreeing to share a large portion of its rare earth minerals deposits with the U.S. as one of a number of conditions for continued American military and economic support of that country.

Despite the caveat that resource scarcity has not been unfolding quite as outlined in the Quagmire scenario, other factors appear to be driving an increase in extremist and maximalist thinking around the globe. In a chapter for the Kingston Consortium on International Security (KCIS) series publication *The (Un)Changing Character of War*, "Observations from Canadian Army Futures Work and the [Un]Changing Character of War: Extremism and Maximalism 2016-2024," Addinall, Dizboni, and Gizewski (2024) considered seven developments over the last decade that we argued were indicative of these trends. The first of these was the election in 2016 of Donald Trump as U.S. President and an associated further increase in the polarization of American politics, an acceleration of a trend that had in some respects been underway since the 1990s. The second was the 2016 "Brexit" referendum in the United Kingdom which led to that country withdrawing from the European Union. The third was the ideologically charged reactions to the COVID-19 pandemic, including a variety of conspiracy theories and anti-vaccine protests in various countries, including Canada. The fourth was the series of decisions of both the Trump and Biden administrations in the U.S. that led to a poorly executed withdrawal of American led forces from Afghanistan and a return of the Taliban to power in that country in 2021. To this can now also be added the takeover of Damascus by HTS in December 2024. The fifth was the full-scale invasion of Ukraine launched by Russia in 2022, expanding the conflict that had started with Russian occupation of Crimea and support to separatists in the Donbas in 2014. Sixth was the Israel-Hamas conflict that began on October 7, 2023, in particular in Gaza, and that, despite ceasefires,

does not appear fully resolved as of early 2025. The seventh was the Yemen civil war that has been ongoing since 2014, and which by 2024 had become intertwined with the Israel-Hamas conflict with Houthi attacks on international shipping in the Red Sea and U.S. and U.K. air strikes against targets in Yemen (Addinall et al., 2024a). In 2025 there is increasing potential for larger scale conflict involving Israel and the US against Iran.

Following up on this work, in a paper for the annual Canadian Political Science Association [CPSA] conference in June 2024 we explored drivers for the trends of increasing extremism and maximalism in more detail. These included both ideational and material drivers associated with the emergence of the internet since the 1990s. The first of the ideational drivers was the appearance of online news sources and the start of a decline in pre-internet forms of mass media (Kaplan, 2025). The second ideational driver was the pattern by which social media began functioning as not only a major source of news for some internet users, but also as another venue conducive to the formation of political and ideological echo chambers. Third was the development of artificial intelligence [AI] algorithms for internet social media and news sources which analyze users' interests and recommend further similar content to them, enhancing the echo chamber effect. We noted that this third ideational driver could be considered a hybrid ideational and material driver, as AI is also a business product designed to increase user engagement and thereby corporate revenues of major technology companies (Addinall et al., 2024b).

We also discussed three material drivers in our CPSA paper. The first of these was a decline in the relative power of the collective West, and the U.S. in particular, at a geopolitical scale. This can be seen as also having an ideational aspect, as it can be argued that this was a perceived as much as a real weakening in the power the West, but it had material causes such as a reduction in the West's share of global GDP, and it had material consequences. The second material driver was a primary consequence of the first; that a decline in the relative power of the West meant that revisionist states – primarily China, Russia, Iran and North Korea – believe that they have opportunities to alter the geopolitical system in the 2020s that they did not have in the 1990s or 2000s. The third material driver that we considered was evidence that revisionist powers seek to further weaken and destabilize the West by taking advantage of subjective factors in the internet age such as the three ideational drivers that we identified above. Examples of this type of intervention, interference, or influence campaign include Russian troll farms and bots that are active on the internet, in particular on social media and in comments sections of online news sources, as well as state-backed online news channels, such as the internet arm of the RT television network, that can also function as propaganda outlets (Addinall et al., 2024b).

Other drivers for extremism and maximalism are likely present, but the important point is that even without unsustainable energy scarcity having (*yet*) fully emerged, many of the characteristics of the Global Quagmire world resemble recent developments. To reiterate, these are, first, a failure to effectively implement solutions to deal with environmental issues at a global scale; second, a zero-sum view of international affairs in many parts of the world; and third, pessimistic, short-term and reactive views of security and how it is achieved. These reflect the Global Quagmire scenario as it was described in the Canadian Army 2015-2017 publications: "Cooperation is muted; conflict, both armed and otherwise, is widespread" (Canadian Army Land Warfare Centre, 2017, p. 24) This analysis of possible future worlds alongside current trends and drivers leads to the next section of analysis in this paper: force structure implications.

Force Structure Implications

Figure 14.2: *Mapping the Four Worlds on the Continuum of Campaign Themes*

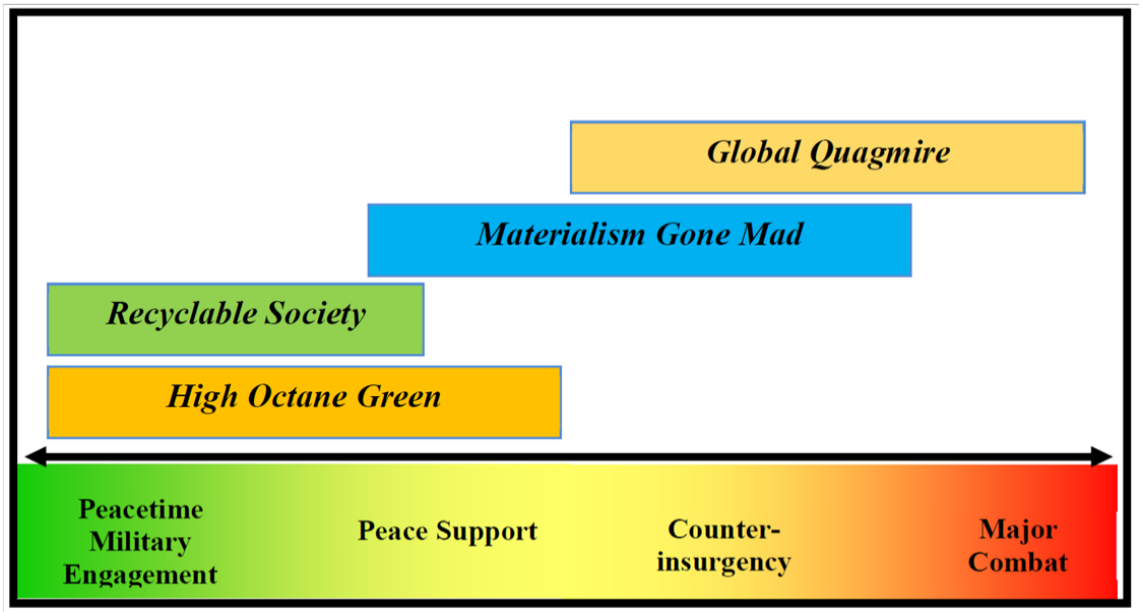


Figure 2: Mapping the Four Worlds on the Continuum of Campaign Themes.

Source:(Gizewski, 2017, p. 7)

As can be seen in Figure 2, more sustainable and proactive worlds may require smaller and lighter force structures. These are described well in a Defence Research and Development Canada (DRDC) Scientific Letter published in 2017 (Gizewski, 2017, p. 7). Moving from left to right across Figure 2, the main points are summarized below.

In a High Octane “Green” World, army missions and tasks become progressively less centred on traditional combat roles, even though the capacity to conduct combat-oriented operations remains necessary. That capability is increasingly overshadowed by missions aimed at maintaining domestic security, protecting national sovereignty, and supporting global stability and sustainability. As economic and social conditions improve, they both require and enable a force that is highly skilled, light-to-medium in weight, rapidly deployable, and environmentally conscious—an evolution captured in Gizewski’s assessment that such a force structure becomes essential in this scenario (2017, p. 8).

In a Recyclable Society, the Army’s missions and tasks are shaped less by armed conflict and more by the overriding imperatives of ensuring domestic and international stability, safeguarding energy security, and promoting environmental conservation. Because energy scarcity and economic decline constrain national resources, military responses tend to be limited in scale and scope. These pressures, combined with the nature of emerging threats and the constraints they impose, point to the need for a light-to-medium-weight force that is oriented more toward domestic responsibilities than external operations. At the same time, the force must be environmentally conscious, reflecting the broader societal shift toward sustainability (Gizewski, 2017, pp. 9–10).

In a world of Materialism Gone Mad, Army missions and tasks reflect a more intense version of the threats and challenges already visible in the mid-2010s—such as terrorism, pressures on sovereignty, and the growing prospect of cyber-attack. These missions generally fall within the middle range of the conflict spectrum, pointing to the need for a medium-to-heavy-weight land force that is adaptive, rapidly deployable, and multipurpose. At the same time, such a force must remain capable of full-spectrum operations to meet the breadth and intensity of emerging security demands (Gizewski, 2017, pp. 7–8).

In a Global Quagmire world, the spectrum of potential threats is exceptionally wide, and these threats are more severe than in any of the other scenarios. The prospects for territorial conquest and the likelihood of both inter-state and intra-state war remain high, creating a security environment defined by persistent volatility. In such conditions, the capacity to generate kinetic effects becomes the central priority for the Army, even as the ability to provide domestic humanitarian assistance, disaster relief, and protection against cyberattack must remain strong. This environment demands a medium-to-heavy-weight force oriented toward missions and tasks at the more intense end of the conflict spectrum, reflecting the elevated risks and operational demands of this scenario (Gizewski, 2017, p. 9).

Accelerating technology change is likely to modify the above suggestions in some respects. In particular, the rapid advancements in drone technology, and mass production of drones, seen in the Russia-Ukraine war from 2022 to 2025 (e.g., Forbes, 2025), as well as the accelerating pace of AI development during the mid-2020s, underscored by mass adoption of generative AI tools such as ChatGPT, is likely to extend and alter what a full spectrum operations force looks like. Nonetheless, his analysis of the force structure implications of the four different types of worlds probably remains broadly accurate.

Conclusion: A High-Tech Quagmire?

The world of 2025 suggests that an additional variation may be emerging that is not captured in the previous analysis of four future worlds. Should resource constraints remain muted while emerging trends nevertheless indicate a continued move to a world resembling Global Quagmire, a plausible future emerges in which the sources of conflict are less driven by the impacts of resource constraints and environmental decay but rather by the trends and drivers highlighted above. This results in military forces less constrained by the limitations on capability which energy scarcity and environmental decline would impose. Rather, extensive spending may take place on both traditional medium-to-heavy force structure equipment alongside new technologies, including automated systems such as drones and anti-drone systems, additional cyber warfare and CIMIC/PSYOPS capabilities to deal with effects on the internet, hypersonic missiles, AI, and many others. This type of emerging scenario might be called the High-Tech Quagmire.[1]

A High-Tech Quagmire world is one in which larger full spectrum forces that incorporate rapidly emerging technologies are likely needed. This likely to be a more expensive force structure to build, maintain, and continually modernize, meaning that pressure on small and medium sized countries, including most NATO countries, to spend over two percent of GDP on defence is likely to increase unless trends change significantly. Indeed, in early 2025 the Trump administration in the U.S. has suggested that NATO countries should spend five percent of GDP on defence, even while it has behaved in ways that suggest skepticism and a possible lack of commitment to the trans-Atlantic alliance (e.g., CBS News, 2025; Foreign Policy, 2025). As previously noted of this paper, threats to the sovereignty of small and medium sized countries are now no longer limited to revisionist powers such as China, Russia, North Korea and Iran. The Trump administration has expressed an interest in annexing Greenland (e.g., BBC, 2025a), and Canada to the United States

[1] Since autumn 2024 a variant of the High Tech Quagmire concept has also been incorporated into future security environment analysis by the Canadian Army Land Warfare Centre following presentation of an earlier version of this paper at the ISMS 2024 Annual Conference. The concept overlaps with, but is not necessarily identical to, the analysis presented here.

(e.g., The Guardian, 2025a; CNN 2025a). It has also withheld military equipment promised to Ukraine by the U.S. Congress and the Biden administration to force that country into negotiations with Russia on a timetable that the Trump administration finds acceptable, as well as to gain greater access to Ukrainian rare earth mineral resources (e.g., CNN, 2025b). It has also threatened to reassert direct control over the Panama Canal (e.g., The Guardian, 2025b; CNN, 2025c; BBC, 2025b), violating Panamanian sovereignty, and has started a global trade war, imposing tariffs on the products of not only opponents such as China, but also of America's traditional allies. Even if a future Democratic Congress, Senate, or Presidential Administration in the U.S. returns to a policy of liberal internationalism and supports the rules-based international order, it is becoming far less likely that any of the world's small and medium sized countries can assume that any of the currently largest powers – the U.S., China or Russia – can be treated as reliable allies (e.g., Chatham House, 2025). Part of this emerging scenario is also that what was described as the future security environment in the 2015-2017 Canadian Future Army process publications is characterized by uncertainty and the inability to make consistently accurate predictions.

The future security environment of 2025 shows all the signs of remaining uncertain, but many features of what was considered the future security environment of the 2010s have already come to pass in what some political scientists, philosophers, sociologists and historians have described as a polycrisis (e.g., Cascade Institute, 2025; World Economic Forum, 2023).[2]

Raising defence expenditures to levels not seen since the Cold War is likely to have significant economic and political culture implications on countries that either cannot, or for many years have had the luxury of choosing not to, spend significantly on defence. Nonetheless, in a polycrisis type global security environment, choosing to respond may become an existential question for many states. Those countries that are perceived as not having a credible capability for self-defence or to maintain security on their own territory and project power to assist allies within their regions may well be seen as illegitimate by the largest powers.

A comparison between two NATO allies, Canada and Poland, is perhaps in some respects illustrative. Canada is an example of a country that could theoretically spend more on defence, but for decades has not. With the benefit of significant geographical distance from major conventional threats, with the oceans on three sides and its longstanding ally the U.S. to the south and in Alaska, the country has spent considerably less than two percent of GDP on defence since

[2] Polycrisis is discussed in many sources, including by historian Adam Tooze, French philosopher and sociologist Edgar Morin, and the Cascade Institute, the founder and executive director of which is Thomas Homer-Dixon who holds a PhD in international relations, defense and arms control policy, and conflict theory. See, for example: https://cascadeinstitute.org/team/ accessed March 13, 2025, and "This is why 'polycrisis' is a useful way of looking at the world right now," World Economic Forum March 7, 2023, accessed March 13, 2025: https://www.weforum.org/stories/2023/03/polycrisis-adam-tooze-historian-explains/

the Cold War. In 2024 the Canadian federal government announced that defence spending will be raised to the NATO guideline of two percent of GDP by 2032 (Department of Defence, 2024). Nonetheless, a skeptic might observe that this is a date sufficiently far in the future that immediate ramifications for other areas of government spending can be avoided. This, in turn, suggests that the Canadian political culture may still be struggling to raise its defence spending to that level – let alone the approximately 3.5 percent that the U.S. spends (Defense, n.d.; World Bank, n.d.),[3] or the 5 percent that the Trump administration has suggested.

By contrast, the Polish foreign minister told Bloomberg Television in July of 2024 that Poland will spend 5 percent of its GDP on defence in 2025 (BNN Bloomberg, 2024). As an eastern European state that borders on close Russian ally Belarus, a country that is controlled by an authoritarian leader, the Poles have likely not felt that they have the luxury of forgetting the long Bloomberg history of invading armies crossing Central and Eastern Europe in previous centuries. Overall, the number of NATO countries spending at or above the 2 percent of GDP on defence has risen since the guideline was established in 2014, from three to 23 (NATO, 2024). Such a contrast between two NATO nations suggests how geopolitical pressure for greater defence spending can continue to increase in a High Tech Quagmire world.

References

Addinall, Robert, & Dizboni, Ali, & Gizewski, Peter. Observations from Canadian Army Futures Work and the [Un]Changing Character of War: Extremism and Maximalism 2016-2024. In Alison Brown and Howard G. Coombs (Eds.), *KCIS 2023: The [Un]Changing Character of War* (pp. 93-111). Queen's University Centre for International and Defence Policy, 2024.

Addinall, Robert, & Dizboni, Ali, & Gizewski, Peter. (2024, June). "Alternative Futures and the Evolving Security Environment Implications for Decision-Makers." Paper presented in Panel C19(b) – Theories of International Relations (IV), 1:45pm - 3:15pm, June 14, 2024, at the Canadian Political Science Association (CPSA) conference, McGill University, Montreal, Quebec, June 12 to 14, 2024.

Aikman, Ian. (2025, January 25). Trump says he believes US will "get Greenland." *BBC*. https://www.bbc.com/news/articles/crkezj07rzro

Axe, David. (2025, March 12). "4.5 Million Drones is A Lot Of Drones. It's Ukraine's New Production Target for 2025." *Forbes*. https://www.forbes.com/sites/davidaxe/2025/03/12/45-million-drones-is-a-lot-of-drones-its-ukraines-new-production-target-for-2025/

Canadian Army Land Warfare Centre. (2015). *Canada's Future Army, Volume 1: Methodology, Perspectives and Approaches*. (Kingston, Ontario: Army Publishing Office).

Canadian Broadcasting Corporation. (2024, August 19). U.S. military announces $20M US grant to build cobalt refinery in Ontario. https://www.cbc.ca/news/world/us-ontario-funding-cobalt-refinery-1.7298973

[3] Statistics vary according to the organization reporting. The U.S. Department of Defense claims that spending may fall below 3% of GDP in 2024 in the online graphic at (Defense, 2025). However, the World Bank, using data from the Stockholm International Peace Research Institute (SIPRI), reports 3.4% of GDP for 2023 in its military expenditures database (World Bank, 2025).

Cascade Institute. (Accessed March 13, 2025). https://cascadeinstitute.org/team/

Collinson, Stephen. (2025, February 21). The Ukraine minerals deal is a perfect metaphor for Trump's foreign policy. *CNN*. https://www.cnn.com/2025/02/21/politics/trump-ukraine-mineral-deal-analysis/index.html

Department of National Defence. (2024, July 11). Statement from Defence Minister Bill Blair on Canada's work to reach the NATO defence investment pledge by 2032. https://www.canada.ca/en/department-national-defence/news/2024/07/statement-from-defence-minister-bill-blair-on-canadas-work-to-reach-the-nato-defence-investment-pledge-by-2032.html

Gizewski, Peter. (2017). Canada's Future Army: Alternative Worlds and Implications. (Defence Research and Development Canada Scientific Letter DRDC-RDDC-2017-L342).

Kaplan, Robert D. (2025) *Waste Land: A World in Permanent Crisis*. New York: Random House.

Lyons, Emmet. (2025, March 7). "Trump questions NATO allies' will for collective defense while casting doubt on U.S.' own treaty commitment." CBS News. https://www.cbsnews.com/news/trump-nato-article-5-collective-defense-europe-doubt-us-treaty-commitment/

North Atlantic Treaty Organization. (2024, June 18). Defence expenditures and NATO's 2% guideline. https://www.nato.int/cps/en/natohq/topics_49198.htm

Oppmann, Patrick. (2025, January 20). Panama turned its canal into a money-maker. History shows why Trump's threats are sounding the alarm bells. *CNN*. https://www.cnn.com/2025/01/20/americas/panama-canal-trump-threat-intervention-intl-latam/index.html

Piotr Skolimowski, (July 13, 2024). Poland to Boost Defense Spending to 5% of GDP, Sikorski Says. *BNN Bloomberg*. https://www.bnnbloomberg.ca/business/international/2024/07/13/poland-to-boost-defense-spending-to-5-of-gdp-sikorski-says/

Roth, Andrew. (2025, January 26). Tension and defiance in Panama after Trump threatens to 'take back' canal. *The Guardian*. https://www.theguardian.com/world/2025/jan/26/panic-and-defiance-in-panama-after-trump-threatens-to-take-back-canal

Sharp, Alexandra. (2025, March 6). "Can Trump's 5 Percent Defense Spending Threshold Save NATO?" *Foreign Policy*. https://foreignpolicy.com/2025/03/06/nato-5-percent-defense-spending-trump-russia-ukraine/

Skolimowski, Piotr. (2024, July 13). Poland to Boost Defense Spending to 5% of GDP, Sikorski Says. *BNN Bloomberg*. https://www.bnnbloomberg.ca/business/international/2024/07/13/poland-to-boost-defense-spending-to-5-of-gdp-sikorski-says/

Stockholm International Peace Research Institute (SIPRI). (Accessed March 13, 2025). https://data.worldbank.org/indicator/MS.MIL.XPND.GD.ZS?locations=US

The Guardian. (2025, March 10). Canada's lonely battle in the face of Trump threats. *The Guardian*. https://www.theguardian.com/world/2025/mar/10/canadas-lonely-battle-in-the-face-of-trump-threats

U.S. Department of Defense. (Accessed March 13, 2025). https://www.defense.gov/Multimedia/Photos/igphoto/2002099941/

Vinjamuri, Leslie (Ed.). (2025, March). *Competing visions of international order: Responses to US power in a fracturing world.* Chatham House.

Wolf, Zachary B. (2025, March 11). Canadians are taking Trump's annexation talk very seriously. *CNN*. https://www.cnn.com/2025/03/11/politics/canada-trump-51st-state-rob-ford/index.html

World Economic Forum. (2023, March 7). This is why 'polycrisis' is a useful way of looking at the world right now. https://www.weforum.org/stories/2023/03/polycrisis-adam-tooze-historian-explains/

Chapter 15: Terrorism in Armed Conflicts: A Breach of Norms or an Element of Strategic Culture as per Example of the Russian Federation and Soviet Union

Maria **Juczewska**, ORCID: https://orcid.org/0009-0000-2328-2600

Abstract:

Ongoing military conflicts require the re-evaluation of existing doctrine and ways of warfare. Preliminary observations from the war in Ukraine beget questions regarding the type of war we may face in the near future. Since 2014, a wide range of measures inconsistent with the law of nations has been used by the Russian Federation in Ukraine even though the concept of war crimes was defined in that law over 75 years ago, with the Soviet Union being one of the parties establishing the definitions. At present, neither the Russian authorities nor armed forces take those rules into account when shaping their military tactics and strategy. The harassment and destruction of civilian population in Ukraine seem to bear the hallmarks of terrorism. Therefore, NATO member states need to fine-tune their warfighting concepts to the situation of conflict in which the regulations of the public international law appear to be purposefully disregarded. The aim of this paper is to analyse whether Russia's use of terror and terrorism in armed conflicts is systematic and could be thus considered an element of Russian strategic culture. The context for this analysis has been provided by the ongoing conflict in Ukraine. Three approaches to the concepts of terror and terrorism are examined. Each of them focuses on a different aspect of these phenomena to provide a comprehensive perspective. The definitions of strategic culture and counterintelligence state are introduced to provide an overarching idea for the inquiry. The continuity of means and methods used by the Russian state against its internal and external enemies is detected through comparison of the conflict in Ukraine to the past conflicts in the Soviet Union. Review of literature and the internet sources reporting on the conflict in Ukraine was conducted to analyse and synthesise information leading to the conclusions concerning the Russia's use of terror and terrorism. The most important point is that the strategic culture of Russian Federation freely resorts to both in order to implement short- and long-term domestic and foreign policy goals. The use of terror and terrorism is characteristic of a counterintelligence state, which Russia has revealed itself to be. Therefore, the Russian military forces should be expected to continue to resort to those methods. The conclusion of this presentation shall discuss broader security implications of this state of affairs for global security architecture.

Keywords: Terrorism, Soviet Union, Russia, State-Sponsored Terrorism

Introduction

Armed forces of the Russian Federation in the war in Ukraine display a clear tendency to attack predominantly civilian targets and civilians in violation of the public international law. Their actions aimed at harassment and destruction of the civilian population are characteristic of this conflict. The aim seems to be the intimidation of inhabitants of Ukraine. More than 10 years have passed since the Crimea was invaded in February 2014. The war has lasted for more than a decade now. In its course, Russian Federation has resorted to a wide array of military measures violating international public law such as systematic torture and extermination of civilians (Der Spiegel, 2023), deportations of underage Ukrainians to the Russian Federation territory and their subsequent Russification (Biuletyn PISM, 2023), attacks on city centres, housing districts and hospitals (PBS, 2024), looting of public and private property (PAP, 2024). Already in 1945, by way of the Charter of the International Military Tribunal in Nuremberg the criteria of accountability for war crimes were established. The Charter has become in this way the cornerstone of the international law in this regard (Gąska, 2003). In the article 6 of the Charter, three categories of crimes that may occur during the conduct of hostilities were defined: crimes against peace, war crimes and crimes against humanity (Gąska, 2003).[4] Majority of thus defined criminal acts has regularly been committed in Ukraine by the Russian armed forces. This means that – even though the concept of a war crime has been clearly defined in the international public law for over 75 years now – neither the authorities of the Russian Federation nor its armed forces take it into account when shaping Russian military strategy or tactics (Gąska, 2003, p. VII). Noticeable tendency displayed by the Russian Federation in the conflict in Ukraine to target military actions against civilians encourages reflection on the role of terror and terrorism in the conflicts conducted by Russian Federation. This article shall probe into the issue of whether the political and military authorities of the Russian Federation consider terror and terrorist acts as legitimate forms of military action used in the battlefield to achieve tactical and strategic goals.

Terror versus terrorism

[4] These include, among others, acts such as preparing, initiating and waging a war of aggression, violations of the laws and customs of war (murder, ill-treatment of the civilian population, deportation of civilians, murder and ill-treatment of prisoners of war, killing of hostages, plunder of public and private property, wanton destruction of residential infrastructure, enslavement, inhumane acts committed against the civilian population before or during the war, persecutions on political, racial or religious grounds) as per Mjr dr Marek Gąska, *Planowanie Operacji Wojskowych w Świetle Międzynarodowego Prawa Humanitarnego Konfliktów Zbrojnych Dokumenty i Materiały Cz. 4 Odpowiedzialność za Przestępstwa i Zbrodnie Wojenne,* Akademia Obrony Narodowej Wydział Strategiczno-Obronny Katedra Prawa i Bezpieczeństwa Międzynarodowego Warszawa 2003 p. VII.

To conduct a well-informed examination of the problem, the difference between the terror and terrorism needs to be briefly discussed by way of introduction. The fact of the two phenomena being intertwined in practice shall be indicated and analyzed in the wider context of Russian Strategic Culture. This analysis shall lead to a conclusion concerning terrorism as an element of the military practices of Russian Federation.

Terror as we understand it today was used for the first time in the period of Jacobin Reign of Terror during the French Revolution (Hołyst, 2009, pp. 68-69). As pointed out by Hołyst in his monumental work *Terroryzm* [Terrorism], in the later stages of the French Revolution (years 1793-94) "the system of terror became an instrument of management created by the revolutionary state" (2009, p. 68). In this revolutionary management concept, the intimidation of the opponents of new regime had become a tool of power consolidation. Hołyst cites after Hoffman the features of modern terror of that era, namely: being organized, purposeful targeting of a group destined for elimination, systematic approach and the intent to create a new better society and a new political system (2009, p. 69).

A question should be asked, however, to what degree present-day terror is akin to terrorism. At present, two approaches in the research on terror and terrorism in the field of social sciences in Poland can be identified. One, which does not differentiate between the two notions, because the ultimate effect of the two phenomena is the same, namely "to instill terror, to infuse consciousness of the victims with extreme fright" (Hołyst, 2009, p. 56). This perspective is closer to the one represented in the English language literature which tends to focus on the identification of the characteristic features of terrorism rather than the elaboration of the theoretical differentiation between terror and terrorism (Hołyst, 2009, p. 61). In this approach, the main features of terrorism entail the use of violence by all available means, targeting innocent civilians, lack of remorse when resorting to brutal violence, the will to instill horror, the wish to achieve political, ideological, military, ethnic or religious goals which often seem irrational to non-terrorists (Hołyst, 2009, p. 61).

The second perspective on terrorism in Polish research focuses on the fact that terror and terrorism differ from one another in terms of the relationship to power and the socio-legal status of the entities involved (Hołyst, 2009, p. 56). Therefore, it defines terror as "brutal violence used by the state apparatus (…) in order for an elite, a small selected group, (*dictatorship*), to remain in power" (Hołyst, 2009, p. 56). Meanwhile, terrorism is understood as, "the use of violence by people acting in strict secrecy against a particular social, political, economic or religious situation – in order to change it" (Hołyst, 2009, p. 57). Violence in such contexts is used in such an intensity that it gains "the capacity to generate the atmosphere of intimidation" (Hołyst, 2009, p. 57). In line with this view, terror might be described as an instrument used by an elite to remain in power, while

terrorism – as an attempt to overthrow the existing elite by an aspiring power group ready to use extreme means to gain it.

In reference to the definitions above, one can analyze the conflict in Ukraine from three angles to verify whether the Russian Federation considers terror and terrorist acts as acceptable forms of armed struggle. First, a historical perspective shall be presented. Then, a perspective based on the English language literature shall be examined. Finally, an approach more popular in Polish social sciences shall be analyzed.

Historical perspective

Although the concept of terror as a method of exercising power appeared first in relation to Jacobin France, it was not the only revolutionary state that used terror in an organized, systematic manner, deliberately selecting groups to be eliminated, with the intention of creating a new, better society and building a new political system (Hołyst, 2009). Soviet Russia at its inception was also such a state. At the root of this state, there lie the October Revolution and the brutal civil war which claimed about 15 million lives (Malia, 1994, p. 137). The most important instrument used by the authorities of the Soviet state in its early days, aimed at forcing the citizens into obedience and maintaining the Bolsheviks in power, was an institution created specifically for this purpose - the All-Russian Extraordinary Commission for Combating Counter-Revolution and Sabotage, the so-called Cheka. This institution then evolved, taking on a number of names and undergoing organizational transformations throughout the history of the USSR (Dziak, 1987, pp. 1-73). John J. Dziak, an American analyst researching Russian intelligence services, presented this process in detail in his monograph *Chekisty: a history of the KGB*. In this work, Dziak defined the USSR as a state based on counterintelligence services (*a counterintelligence state*)[5] (1987, p. 3). The main purpose of such a state is to combat alleged internal and external enemies in order to serve the interests of the elite of this country recruited from among members of the ruling party (*usually with a revolutionary program*) and security organs (Dziak, 1987, pp. 1-3). Despite the political transformation and the fall of the USSR, the Russian Federation continues to meet the criteria of

[5] Given the ubiquity of influence of state security agencies in Russia, the term secret police state could also be appropriate to describe the *modus operandi* of the Russian state. However, the term counterintelligence state seems to be more adequate a choice for the sake of a scholarly debate destined also for audiences less familiar with the Russian strategic culture and history. Firstly, because it makes the idea of such a political arrangement within a state more approachable to Western audiences. Secondly, because it draws attention to the particular type of methods employed by this state's securitized administration to wield and preserve power. These methods are being used by a plethora of security agencies (widely referred to as "organs" by the Russian population) to oppress and control the societies of Russian Federation as well as subjugate the societies in the countries with which Russian Federation is at war. However, for the sake of the very scholarly debate, it needs to be made clear here, as per recommendation of Erik Heldna, Estonian Military Academy, that the counterintelligence agencies of NATO or the EU differ radically from the Russian security services such as the FSB. The primary function of the latter is not to protect legitimate national interests or gather intelligence on external threats but rather to use covert methods to suppress internal dissent and opposition. Furthermore, Russia employs the GRU (military intelligence) for similar repressive and terrorist purposes, although it is not a counterintelligence agency (clarification courtesy of Eerik Heldna, Estonian Military Academy).

the definition above. Russian methods of warfare at the end of the 20th and beginning of the 21st century (*the Chechen wars, the war with Georgia, the war in Ukraine*) provide additional evidence confirming the accuracy of Dziak's definition. The course of the war in Ukraine illustrates that the Russian armed forces do not hesitate to resort to methods used by counterintelligence organs, brutally intimidating and eliminating civilians, in addition to facing Ukrainian soldiers in the battlefield. The most drastic example of such actions by the Russian armed forces was the systematic massacre of the population of Bucha occupied by the Russians between March 5 and March 28, 2022 (UN Human Rights Commission, 2022). In addition, the current Russian authorities openly draw on the models and experiences of the USSR period in their historical policy (Darczewska, 2015, pp. 59-73), and political rhetoric (McGlynn, 2024). People who openly question the actions of Russian elites are eliminated in a brutal and spectacular way, like Anna Politkovskaya (Stempin, 2024), Boris Nemtsov (Bieliaszyn, 2024), or Aleksandr Litvinenko (PAP, 2024). One can therefore assume that terror as a tool for consolidating and maintaining power is still a method of action generally accepted by the ruling elites of the Russian Federation both in times of peace and in times of war.

Moreover, it seems that terror as a method of consolidating power has been used in the history of the Russian Federation and the state entities preceding it for so long that resorting to it has become a legitimate choice also in the eyes of the entire Russian society. That is, terrorizing has become an element of the strategic culture of the Russian Federation. Strategic culture reflects "ways of thinking and acting in relation to power that have their roots in the perception of national historical events and other unique experiences of society related to geography, political philosophy and practice, civic practice, and lifestyle" (Gray, 1986, p. 36). To illustrate what the Russians think about their military's actions in Ukraine, including the use of terror in this conflict, it is worth looking at the language used to describe it. The term Special Military Operation is of particular significance here. It appeared in Russian propaganda channels along with the escalation of hostilities in Ukraine in 2022. Commentators see this term as a crude euphemism or an attempt to avoid a formal declaration of war by the Russian Federation so that the rules and regulations of the international public law could not apply in the cases of human rights' violations in Ukraine (Dubianskij, 2022; Kolesnikov, 2023). However, the term also has deeper cultural connotations. Commentators note that the word 'operation' in Kremlin jargon means a military intervention in an area considered to be within Russia's sphere of influence. Thus, the Chechen wars were described as an "anti-terrorist operation" and the Russian-Georgian war as a "peace-enforcing operation" (Dubianskij, 2022). However, the term 'operation' has a much longer history. Namely, all organized repressive actions targeted against specific nations of the USSR, including genocides of entire

ethnic groups, were called operations. For example, the German operation, i.e. the action of expelling the Volga Germans in 1937, or the Polish operation, i.e. the first ethnically motivated genocide in the USSR, in which between 111,000 and 200,000 Poles living in the USSR were killed in the years 1937-38 (Sommer, 2014, pp. 347-371). By analogy with the earlier usage of the term 'operation' in Russian history, we may assume that this word has gained a particular sense according to the strategic culture of the Russian Federation. Namely, for citizens of the Russian Federation it has become a synonym for repressive actions against the local population aimed at least at ethnic cleansing.

A particular language of Russian propaganda regarding the conflict in Ukraine is also worth noting here. This propaganda primarily targets residents of the Russian Federation and is characterized by the references to the era of Nazism and World War II. A detailed content analysis of messages regarding Ukraine and its inhabitants broadcast in the Russian information sphere would require a separate study. However, we can cite here the main lines of the Kremlin's anti-Ukrainian rhetoric, on the basis of selected documents. For example, Timofey Sergeytsev's text *What Russia Should Do with Ukraine* published by RIA Novosti on April 3, 2022 denies the right to national identity to Ukrainians, accusing them of supporting fascism (*both the government and the citizens*) (Forsal, 2023); dehumanizes an ordinary citizen through the usage of pejorative terms; and calls for the "denazification of Ukraine" by means of "de-Ukrainization" and "de-Europeanization" (Forsal, 2023). According to an expert from the Centre for Eastern Studies interviewed by Forsal, Maria Domańska, so aggressive a propaganda language signals a transition from an authoritarian to a totalitarian form of Vladimir Putin's rule (Forsal, 2023). While she compared this language to Nazi genocidal propaganda, it also parallels the language of Soviet anti-Polish propaganda from the interwar period and World War II, especially when it comes to the accusation of supporting fascism and alleged collaboration with fascist regimes (Forsal, 2023). This accusation was regularly brought up by the USSR against the government of the Second Polish Republic before the WWII as well as against soldiers of the Polish independence underground during and after the WWII (Sommer, 2014, pp. 202-203). Just as Ukrainians today are presented as an ethnic element that needs to be terrorized and subjected to forceful Russification, Poles in the USSR in the 1930s were deemed to be spies unworthy of the Soviet citizenship, "White Poles" who oppressed proletarians and deserved the death penalty (Sommer, 2014, p. 94). The aim of such linguistic manipulations is to demonize and dehumanize a group that until recently was presented as part of a larger Russian-speaking community. Excerpts of telephone conversations between Russian soldiers and their families intercepted by intelligence services of other countries or snippets of recordings from surveillance cameras from Bucha provide

evidence of how effectively propaganda shapes the perception of citizens of the Russian Federation (e.g. PBS, n.d.). The recordings reflect the perspective of Russian propaganda, in which both a Ukrainian soldier and a civilian is the enemy deserving to die if they oppose Russian conquest, notwithstanding the non-combatant status of the latter (Associated Press, n.d.d).

As can be seen, adopting the criteria of the historical perspective, the conduct of the Russian Federation authorities and the Russian Armed Forces during the conflict in Ukraine can be described as an attempt to consolidate and maintain power in the new territory by a state of revolutionary origin based on counterintelligence services using terror in an organized, systematic manner, deliberately selecting groups to be eliminated (*representatives of local authorities, male Ukrainians, men and boys alike*) (UN Human Rights Commission, 2022), with the intention of creating a new society and building a new political system.

English language literature's approach

English language research on terrorism seems to be focused on defining what terrorism is in practice. NATO Glossary Of Terms And Definitions defines terrorism as "the unlawful use or threatened use of force or violence against individuals or property in an attempt to coerce or intimidate governments or societies to achieve political, religious or ideological objectives" (NATO, n.d.). According to this approach, the main features of terrorism entail the use of violence by all available means, targeting innocent civilians, lack of scruples in using brutal violence, the desire to sow terror, the desire to achieve political, military, ethnic, ideological or religious goals that are often irrational for non-terrorists (Hołyst, 2009, p. 61). As to the use of violence by all available means, it is undoubtedly present in this conflict on the part of the Russian Federation. It was already noted in the introduction to this work that a characteristic feature of this conflict is the frequent violation of public international law whose aim is to sow terror. Violence is used not only against combatants, but also to a large extent against innocent civilians (*bombardment of city centers and residential areas, hospitals, schools and universities*) (PBS, 2024). Repressive actions against civilians are characterized by a lack of scruples in the use of brutal violence (*torture chambers discovered in Kherson, extermination of the population of Bucha*) (PAP, 2024). An interesting criterion in this perspective is the "desire to achieve political, military, ethnic, ideological or religious goals that are often irrational for non-terrorists" (Hołyst, 2009, p. 61). The attempt to Russify Ukrainian children appear to meet this requirement. This procedure has been ongoing since the very beginning of the war in 2014 and concerns both Ukrainian war orphans and children whose parents are still alive (PAP, 2023). The cases of deportation of Ukrainian children from cities occupied by the Russian Federation are widely documented (Associated Press, n.d.a; Associated

Press, n.d.c). The process of their Russification, presented as a generous rescue of children from war, is one of the topics of propaganda addressed to residents of the Russian Federation (Kolesnychenko, 2023). Although these practices are contrary to public international law, the Russian Federation does not stop the deportation and denationalization of Ukrainian children. If we have a look at these actions from the perspective of the children who do not want to become citizens of Russia, or their parents who are still in Ukraine, we can consider them incomprehensible. They will become understandable only if we accept the Russian Federation's point of view that war or victory in war means also ethnic cleansing in the conquered territories. This proposal, in light of the legal rules and regulations in NATO countries, is completely irrational and impossible to accept as contrary to public international law *(deportations constitute a violation of the laws and customs of war*) (e.g. Gąska, 2003).

Another spectacular example of a situation in which the Russian authorities decided to take military action, which brought benefits disproportionate to the negative consequences for the Ukrainian population, was the flood caused by the Russian troops' having blown up the dam in the lower reaches of the Dnieper in the town of Nova Kakhovka in June 2023. The very idea of causing a flood and destruction of the environment over a huge area can be treated as an example of thinking that does not fit into rational categories in the understanding of Western civilization. One might be tempted to try to draw an analogy between this act and the British Operation Chastise on 17th May 1943, when the destruction the Möhne and Eder dams (*2 out of 5 destined for destruction in this operation*) by the British paralyzed certain sectors of German industry within the Ruhr Valley (Kiras, 2006, pp. 35-57). However, the difference between the two acts becomes clear when they are analysed in light of the concept of just war, which puts forward the rule of conduct when entering (*jus ad bellum*) and conducting (*jus in bello*) war. Jus in bello stipulates, among others, proportionality of force, whereby the harm to civilians or their property caused by a military action cannot be excessive in relation to the direct miliary advantage anticipated as a result of an attack on a legitimate military target (Childress, 2025, p. 33). The idea behind the Operation Chastise was to strike the dams in the Ruhr Valley, which produced energy for the majority of German industrial production in order to deal a decisive blow to the German military industry and thus end WWII. The dams became the target, because they provided energy for the crucial industrial area of the aggressor with the hope that this was going to be a strategic move ending the global war. Such radical and deadly operations may well seem to be justified in the face of a global conflict. Meanwhile, resorting to the destruction of the dam in Nova Kakhovka to slow down the retreat of the Russian forces in the area, with no clear military target to destroy in the close vicinity of the dam (unless the nearby Zaporizhzhia Nuclear Power Plant could be considered a legitimate

military target) by way of a formidable flood seems disproportionate to the gravity of the regional conflict – or the "special military operation", for that matter. Even if Russian propaganda ascribes higher order of magnitude to this conflict, it is still perceived as a conflict of regional scale by major international organizations (e.g. Atlantic Council, 2022; Veterans Today, 2022). What is more, putting in peril the Ukrainian civilians and the very Russian troops present in the area alike underscores the disregard for human life characteristic of the Soviet conduct of wars. The behavior of the Russian soldiers and the Russian civilian administration in the occupied territories in the face of this man-made natural disaster can be considered yet another example of irrational thinking, which assigns higher priority to propaganda activities (*denying that the flood had been caused by human activity or that it posed a threat to the inhabitants in the area*) than to saving human lives. The Russian administrative authorities on the left bank of the Dnieper occupied by the Russian Federation not only did not undertake rescue operations for the local population but also prohibited the registration and burial of the dead. They also significantly underestimated the number of victims and abducted some of the bodies (Associated Press, 2023b).

The analysis of the conflict in Ukraine in line with the criteria of terrorism enumerated in the English-language scholarly literature – the use of violence by all available means and without scruples, targeting innocent civilians, the desire to sow terror, the desire to achieve political, military, ethnic, ideological or religious goals that are often irrational for non-terrorists – shows that the actions of the Russian military on the territory of Ukraine can be considered terrorism. In the occupied areas in Ukraine, the Russian Federation engages in practices that are characterized by exceptional brutality and lack of inhibitions in the act of large-scale destruction of human and material resources. What is more it is enabled by the efficient cooperation of Russian law enforcement and military organs with administrative and political authorities of the Russian Federation in the occupied area. The element of forceful pursuit of goals that are irrational from the point of view of non-terrorists is particularly important here. If Ukrainians are to survive as a nation, they possibly cannot agree to the Russian vision of Ukraine as a dependent territory, whose recalcitrant inhabitants should be forced through terror to recognize the authority of the Russian Federation, whose children are to be deported into the territory of the Russian Federation in the grand ethnic cleansing scheme, and whose country's key infrastructure, agricultural areas and human resources are to be deliberately destroyed.

In addition, the horrific experiences of World War II and the Nuremberg Trials have set the criteria for what the Western world considers rational behavior, even in times of an armed conflict. The conflict in Ukraine proves that the strategic culture of the Russian Federation does not respect any norms regarding the conduct of members of the armed forces at war, which were established

in the international forum after World War II. Although the Russian Federation has not ratified the Rome Statute and therefore is not subject to the jurisdiction of the International Criminal Court in The Hague (Kuczyńska, 2022), the Soviet Russia was one of the four signatories to the London Agreement. This agreement established the International Military Tribunal in Nuremberg, which defined three types of crimes for which war criminals can be held accountable (Stankiewicz, 2006, p. 146). It is therefore clear that as early as in 1945, the Russian authorities were able to reach an agreement with the other states that signed the charter on the definition of war crimes. Consistent disregard of the norms previously established by one's own state can therefore also be seen as irrational behavior on the part of both the authorities of the Russian Federation and representatives of its armed forces.

Polish social sciences' view

It is now necessary to recall the definitions of terror and terrorism presented earlier in this work. Terror according to Hołyst is "brutal violence used by the state apparatus (...) in order to maintain power, which is usually exercised by a narrow group, an elite (a dictatorship)" (Hołyst, 2009, p. 56). This is precisely how the occupation authorities of the Russian Federation and its armed forces act in the territories they occupy. Additionally, as in the times of the Great Terror, the armed forces of the Russian Federation behave more like counterintelligence units, using a range of measures traditionally used by Soviet counterintelligence against citizens of the USSR and the countries it occupied – organizing deportations, torture, planned physical elimination of men and persecution of civilians. What is particularly striking is the similarity of the Russian soldiers to the People's Commissariat for Internal Affairs [NKVD] functionaries from the time of the Great Terror. Their main activities, apart from common plunder, are intimidating and killing civilians with complete disregard for public international law.

Here an interesting question arises – does a modern soldier of the Russian Federation who, in accordance with the orders of his superiors, uses measures prohibited by public international law against civilians automatically become a terrorist or does he remain merely a soldier of the armed forces of his country, waging war in accordance with the specific strategic culture of his country and nation? To answer it, the definition of terrorism by Hołyst will be reminded, i.e. "terrorism is the use of violence by persons acting in strict conspiracy against a specific social, political, economic or religious situation – in order to change it" (2009, p. 57). While at this stage of the conflict the Russian Federation troops are present in full uniform, in 2014, during the occupation of Crimea, an important role was played by unmarked sabotage units, the so-called "little green men" (Wilk, 2023; Wojnowski, 2015, p. 11). Since the beginning of the Ukrainian-

Russian conflict, the presence of FSB officers in the Donbas region, performing organizational and disciplinary roles in the Donetsk People's Republic, has been proven (Żochowski, 2015, p. 80). In Ukraine, therefore, violence is being organized and used by people acting in strict conspiracy against a specific political situation in order to change it, because representatives of the internal security services of the Russian Federation cooperate with regular soldiers of the armed forces of the Russian Federation, conducting a number of sabotage actions and organizing control over the conquered Ukrainian territories using terror. This happens with the acceptance and cooperation of the regular armed forces of the Russian Federation, which do not take into account the regulations of public international law. The camouflaged participation of the security services of the Russian Federation in the war in Ukraine also delayed the reaction of the Ukrainian authorities, who, trying to respect the civil liberties of Ukrainian citizens, had not managed to stop in time the actions inspired by the Russian services aimed at separating a part of the territories of Ukraine from the rest of the country (Wrzosek, 2018, p.351).

When discussing the definition of terrorism developed in the Polish language literature, it should be noted that “acting in strict conspiracy against a specific political situation in order to change it” can be identified on the part of the Russian Federation in this conflict not only at the tactical level, but also at the strategic level (Hołyst, 2009, p. 57). To this day, the Russian Federation has not declared war on Ukraine, nor does it refer to its actions on the territory of Ukraine as war, but as a Special Military Operation. The Russian Federation authorities have undertaken long-term actions aimed at transforming the border regions of Ukraine into puppet, seemingly independent Donetsk and Luhansk People's Republics, in order to then annex them to their territory at the next stage of the conflict. Similar actions had been undertaken in Crimea, taking advantage of the ethnic predominance of Russians in these areas. Therefore, the methods of action of the political authorities and decision-makers of the Russian Federation also meet the criteria of terrorism proposed in Polish literature.

The Poisoned Well

Jolanta Darczewska, a renowned Polish expert on Russian affairs and Russian security forces, has made an interesting point in relation to the Russian strategic culture. In her 2015 analysis entitled *The Devil Is In The Details. Information Warfare In The Light Of Russia’s Military Doctrine* of the Russian military doctrine of 2014, she focused on the notion of information warfare as presented by the doctrine (Darczewska, 2015a). One of the main conclusions of the analysis is that the Russian doctrine of the information warfare has not changed in essence since Soviet times. It relies on a plethora of methods that have been used and perfected since the 1920s by the

Soviet intelligence and counterintelligence services, such as "sabotage, diversionary tactics, disinformation, state terror, manipulation, aggressive propaganda, exploiting the potential for protest among the local population" (Darczewska, 2015a, p. 7). What changed is the vocabulary used to refer to those methods, as the Russia's Military Doctrine borrowed the notions from the Anglo-Saxon theories describing the new type of war (*asymmetric, non-contact, indirect*) and adapted them to Russian conceptual framework. According to Darczewska, in this way, the Anglo-Saxon terms not only mask the true meaning of the Russian terms but also create a false sense of affinity between the Russian and the Western methods of combat to mislead Western experts (Darczewska, 2015a, p. 7). Especially given that the authorities of both NATO and European Union member states still debate on the scope of the notions related to dynamic development of the cyber domain of military conflicts and various type of subversive actions enabled by the internet, for instance "irregular warfare" or "hybrid tactics" (Marsili, 2023). The analysis made one particularly intriguing point in view of the escalation of war in Ukraine in 2022. Namely, it pointed out that already in 2010 (*when the previous iteration of the Russia's Military Doctrine had been published*), the chapter entitled "*The Leading Role of the Russian Armed Forces in the Military Policy of the Russian Federation*" disappeared from it. According to the expert, this disappearance signalled that civilian military formations are to become the key actors responsible for the implementation of the so-called non-military methods of struggle defined in this very doctrine (Darczewska, 2015, pp. 20-21). The fact that a wide array of measures traditionally used by Soviet counterintelligence services to subdue civilian population was employed in the occupied territories of Ukraine after the escalation of the conflict in 2022 suggests the participation of Russian civilian military formations in the preparation of these acts, at least at the conceptual level, in line with the Darczewska's insight from the 2015 analysis.

In the chapter discussing irregular warfare in *Modern Strategy*, Colin S. Gray remarks that the phenomenon of guerilla warfare in the conflicts of the 20th c. inspired the nascence of "regular troops organized, trained, equipped, and directed to wage war unconventionally in what have come to be known as 'special operations' (Gray, 1999, p. 286). Numerous cases of Russian troops misconduct in the war in Ukraine combined with the provisions of the Russian Military Doctrine point indeed to the unique role of civilian "special forces" in the Russian strategic culture. As based on the examples discussed, these troops seem to complement the military activities of the regular Russian troops, administering the occupied territories and unleashing terror upon civilians in order to stabilize the conquered territory. Further discussion of Mao Tse-Tung's concept of revolutionary warfare in Grey (1999, pp. 292-293) points to other noticeable affinities with the Russian conduct of war in Ukraine. In his doctrine, Mao stressed three important points. Firstly, he emphasized the

need to support the guerilla movement with a political organization (Grey, 1999). This political organization, the amalgam of the members of the revolutionary ruling party and the state security organs, have been in place for more that a hundred years now, as posited by the concept of counterintelligence state by Dziak. Secondly, Mao divided revolutionary warfare into three subsequent stages – political organization, guerilla operations, and the final stage – transition to regular operations of war leading to a decisive battle, because guerilla warfare as such does not deliver victory but undermines the resilience of the attacked and saps the will to defend oneself; presently, the war in Ukraine may probably be said to have reached stage two (*former autonomous people's republics of Luhansk and Donetsk politically organized as parts of Russian Federation, occupied territories in the process of being subjugated by terror unleashed by military and civilian Russian forces*) (Grey, 1999). Thirdly, Mao warned that a revolutionary war is likely to become a protracted conflict, therefore the revolutionaries waging it need to be prepared for a long confrontation (Grey, 1999). By this point, this confrontation has continued for 11 years. What is innovative in the Russian approach to the war in Ukraine in light of the Mao's concept of the revolutionary warfare is that a general war is complemented by an irregular war/terrorism. Two types of war are waged in concert, in order to achieve strategic goal of complete subjugation of Ukraine and its nation.

When probing into the sources of exceptional level of violence against civilians in a war waged by a counterintelligence state, one more revolutionary writer needs to be inspected. In the collected works of Vladimir Lenin, there is a brief chapter devoted to guerilla warfare. After a short discussion of the history of revolutionary struggle in Europe and in Russia, Lenin moves on to the discussion of the armed struggle of a revolutionary. And so he states:

> "Armed struggle pursues two different aims, which must be strictly distinguished: in the first place, this struggle aims at assassinating individuals, chiefs and subordinates in the army and police; in the second place, it aims at the confiscation of monetary funds both from the government and from private persons. The confiscated funds go partly into the treasury of the Party, partly for the special purpose of arming and preparing for an uprising, and partly for the maintenance of persons engaged in the struggle we are describing. (…) The intensification of the political crisis to the point of an armed struggle and, in particular, the intensification of poverty, hunger and unemployment in town and country, was one of the important causes of the struggle we are describing. This form of struggle was adopted as the preferable and even exclusive form of social struggle by the vagabond elements of the population, the lumpen proletariat and anarchist groups. Declaration of martial law,

> mobilisation of fresh troops, Black-Hundred pogroms (Sedlets), and military courts must be regarded as the "retaliatory" form of struggle adopted by the autocracy" (Lenin, 1962).

It is quite clear that 'armed struggle' is a code name for armed robbery, which Lenin justifies as long as it is performed by revolutionary elements, even if robbing others at gunpoint is the only revolutionary activity they perform. At the same time, Lenin encourages murdering of police and military officers and expresses his support for problematic social groups (*vagabonds, the poorest city dwellers, anarchists*) who undermine order and social cohesion, denouncing legal measures aimed at curbing crime. Further in the same chapter, Lenin declares that the main problem is not that the armed robberies take place at all, but that the party does not exercise full control over them. At the same time, it is clear that Lenin has no intention of either removing incentives to steal or to stop the robberies, because they are a necessary element of the revolution:

> It is not guerrilla actions which disorganise the movement, but the weakness of a party which is incapable of taking such actions under its control. That is why the anathemas which we Russians usually hurl against guerrilla actions go hand in hand with secret, casual, unorganised guerrilla actions which really do disorganise the Party. Being in capable of understanding what historical conditions give rise to this struggle, we are incapable of neutralising its deleterious aspects. Yet the struggle is going on. It is engendered by powerful economic and political causes. It is not in our power to eliminate these causes or to eliminate this struggle. Our complaints against guerrilla warfare are complaints against our Party weakness in the matter of an uprising (Lenin, 1962).

As demonstrated above, the main ideologue of the communist party proposed an ideal of revolutionary "struggle" which by way of undermining the current social order through assassination of policing forces, violent robbery and promotion of the most reckless social groups is to serve economic and political causes of building a new order (Lenin, 1962). In this new order, the revolutionary party shall exist to consume appropriated funds and arm itself and prepare for future uprising. Such is the original ethos of the Russian revolutionary. The code of conduct of a Russian revolutionary, military or civilian, has been founded on anti-values since its inception. It is hardly surprising that these anti-values are reflected by the Russian military doctrine and the conduct of wars with a pronounced tendency to resort to disproportionate offensive means and deploy terror against civilians.

Conclusion - Terrorism as a key warfare in Ukraine

As discussed above, the actions of the armed forces of the Russian Federation and representatives of its administrative authorities in the occupied territories of Ukraine meet the criteria of terrorist activities in the understanding of the three analyzed perspectives It can therefore be stated that the thesis put forward at the beginning of this work has been confirmed: the political and military authorities of the Russian Federation treat terror and terrorism as acceptable forms of armed struggle used to achieve both tactical and strategic goals in the war in Ukraine. This is due to historical and institutional continuity with the USSR, and especially due to the fact that the Russian Federation can be described as a state based on counterintelligence services. The specific way of perceiving political reality by representatives of these services seems to result in a selection of particular methods of action at the strategic and tactical level. On the one hand, these are long-term, camouflaged sabotage actions at the initial stage of the conflict, on the other hand, a preference for brutal methods and terror during the escalation of the conflict, especially against the civilian population. Both of these methods of conduct meet the criteria of terrorism according to the analyzed perspectives. Interestingly, the armed forces of the Russian Federation reflect the organizational culture of Russian security agencies, recognizing the primacy of force and terror over international public law.

An interesting aspect of the analysis was the examination of the situation in Ukraine in the light of the criterion of an attempt to introduce by force political, military or ethnic solutions irrational from the point of view of a non-terrorist. A number of actions by the armed forces and authorities of the Russian Federation in the occupied territories of Ukraine prove that the Russian Federation is aiming at ethnic cleansing in the territory it occupies by deporting Ukrainian children to Russia and destroying the adult Ukrainian population on a large scale. This drive to destroy the local population, which can in no way be considered rational from the point of view of the representatives of the Ukrainian nation, emphasizes that the methods of conquest chosen by the Russian Federation in Ukraine are deeply irrational in the light of the norms of Western civilization.

Additionally, Russian strategic culture has been rooted in the Leninist concept of revolutionary warfare which proposes a code of conduct based on anti-values. Informed by the extreme experiences of the revolutionary warfare in Soviet Russia and Maoist China, Russian Federation displays original strategic approach in the conduct of war in Ukraine coordinating in fact two complementary types of war: a regular war and systematic intimidation of civilians through disproportionate use of violence and terror.

Damian Jarnicki in the monograph entitled *Rosyjska wizja współczesnej globalnej architektury bezpieczeństwa* (*Russian Vision of the Contemporary Global Security Architecture*) notes that the Russian Federation, striving to rebuild the global security architecture, aspires to

many roles in the international arena that will allow it to increase its influence on the course of world politics in order to weaken the position of the United States as hegemon. One of those parts is the role of a potentially highly qualified, determined and effective ally in the fight against terrorism (Jarnicki, 2023, pp. 476-477). The true paradox is that by conducting military operations in Ukraine, which has also been aimed at changing the political balance in the region and returning to the group of powers co-deciding on the fate of the world, the Russian Federation has revealed the true nature of its regime, based on the Leninist cult of force and terror, systematically using terrorism as a form of combat against the population of the attacked country. Russian declarations of concern for a more balanced GSA remain in sharp contrast to the methods by which this balance is being achieved on the battlefield in Ukraine. The methods meticulously developed and presented in the subsequent editions of Russian Military Doctrines, as signalled by Darczewska (2015). Meanwhile, no state whose strategic culture is based on terror and terrorism will be able to accept in the long run a role other than... that of another hegemon.

Reference

Amann, M., Gebauer, M., & Schmid, F. (n.d.). *German intelligence intercepts radio traffic discussing the murder of civilians*. Der Spiegel. https://www.spiegel.de/international/germany/possible-evidence-of-russian-atrocities-german-intelligence-intercepts-radio-traffic-discussing-the-murder-of-civilians-in-bucha-a-0a191c96-634f-4d07-8c5c-c4a772315b0d

Atlantic Council. (2022, February 24). *Putin's war speech on Ukraine: Full text and analysis*. https://www.atlanticcouncil.org/blogs/new-atlanticist/markup/putin-speech-ukraine-war/

Associated Press. (n.d.). *Frontline / PBS: War Crimes Watch internet report*. https://www.pbs.org/wgbh/frontline/interactive/ap-russia-war-crimes-ukraine/stories/

Associated Press. (n.d.a). *More Ukrainian children from Ukraine's Russia-held regions arrive in Belarus despite global outrage*. https://apnews.com/article/belarus-russia-ukraine-war-children-6d8c5511b36030d9a361a3a5baf7fc77

Associated Press. (n.d.b). *Russia covered up and undercounted true human cost of floodings after dam explosion, AP investigation finds*. https://apnews.com/article/russia-ukraine-war-dam-collapse-kakhovka-kherson-daacdc431f42912dfb91548794f03a3a

Associated Press, El Deeb, S., Shvets, A., & Tilna, E. (n.d.c). *How Moscow grabs Ukrainian kids and makes them Russians*. https://apnews.com/article/ukrainian-children-russia-7493cb22c9086c6293c1ac7986d85ef6

Associated Press, Kinetz, E. (n.d.d). *'Never saw such hell': Russian soldiers in Ukraine call home*. https://apnews.com/article/russia-ukraine-war-intercepts-2b14732d88b3f58d4a9d0b2b562bdb28

Bieliaszyn, W. (2024, January 18). *Sprawa zabójstwa Niemcowa wciąż czeka na wyjaśnienie*. Polityka. https://www.polityka.pl/tygodnikpolityka/swiat/1943882,1,sprawa-zabojstwa-niemcowa-wciaz-czeka-na-wyjasnienie.read

Biuletyn PISM. (2023). *Deportacja ukraińskich dzieci do Rosji*. https://www.pism.pl/publikacje/deportacja-ukrainskich-dzieci-do-rosji

Childress, J. F. (2025, March 31). Just-war theories: The bases, interrelations, priorities, and functions of their criteria. *Military's Chaplaincy Review, 33*.

Darczewska, J. (2015a, May 19). *The devil is in the details: Information warfare in the light of Russia's military doctrine*. Ośrodek Studiów Wschodnich. https://www.osw.waw.pl/en/publikacje/point-view/2015-05-19/devil-details-information-warfare-light-russias-military-doctrine

Darczewska, J. (2015b, October). *Wojna informacyjna Rosji z Zachodem. Nowe wyzwanie? Przegląd Bezpieczeństwa Wewnętrznego ABW, Specjalne wydanie „Wojna hybrydowa"*, 59–73. https://abw.gov.pl/download.php?s=18&id=3400

Dubianskij, M. (2022, September). *The international law of war and Russia's 'special military operation'*. Global Risk Insights. https://gobalriskinsights.com/2022/09/the-international-law-of-war-and-russias-special-military-operation/

Dziak, J. J. (1987). *Chekisty: A history of the KGB*. Lexington Books.

Gąska, M. (2003). *Planowanie operacji wojskowych w świetle międzynarodowego prawa humanitarnego konfliktów zbrojnych: Dokumenty i materiały. Cz. 4. Odpowiedzialność za przestępstwa i zbrodnie wojenne*. Akademia Obrony Narodowej.

Gray, C. S. (1986). *Nuclear strategy and national style*. Hamilton Press / Abt Books.

Hołyst, B. (2011). *Terroryzm*. Lexis Nexis.

Jarnicki, D. (2023). *Rosyjska wizja współczesnej globalnej architektury bezpieczeństwa*. Wydawnictwo Naukowe UwS.

Kiras, J. D. (2006). Special operations and terrorism: From WWII to the war on terrorism. In *Routledge*, 35–57.

Kolesnychenko, T. (n.d.). *Teraz to są nasze dzieci*. Wirtualna Polska. https://wiadomosci.wp.pl/teraz-to-sa-nasze-dzieci-6891680507685440a

Kolesnikov, A. (2022, December). *How Putin's "special military operation" became a people's war*. Carnegie Endowment. https://carnegieendowment.org/politika/89486

Kuczyńska, H. (2022). Odpowiedzialność przed międzynarodowym trybunałem karnym za zbrodnie prawa międzynarodowego popełnione w czasie konfliktu w Ukrainie. *Palestra, (4).* https://palestra.pl/pl/czasopismo/wydanie/4-2022/artykul/odpowiedzialnosc-przed-miedzynarodowym-trybunalem-karnym-za-zbrodnie-prawa-miedzynarodowego-popelnione-w-czasie-konfliktu-w-ukrainie

Lenin, V. I. (1962–1972). *Collected works* (Vol. 11). From Marx to Mao Digital Reprint. https://ia601606.us.archive.org/22/items/LeninCW/Lenin%20CW-Vol.%2011.pdf

Malia, M. (1994). *The Soviet tragedy*. The Free Press.

Marsili, M. (2023). Guerre à la carte: Cyber, information, cognitive warfare and the metaverse. *ACIG, 2*(1). https://doi.org/10.60097/ACIG/162861

McGlynn, J. (2024, January 20). *The real story behind Russia's new 'Stalin Centers'*. https://edition.cnn.com/2024/01/20/opinions/new-stalin-centers-russia-putin-mcglynn/index.html

NATO. (2023). *NATO glossary of terms and definitions*. https://www.jcs.mil/Portals/36/Documents/Doctrine/Other_Pubs/aap6.pdf

OHCHR. (2022, December). *UN report details summary executions of civilians by Russian troops in northern Ukraine*. Office of the High Commissioner for Human Rights. https://www.ohchr.org/en/press-releases/2022/12/un-report-details-summary-executions-civilians-russian-troops-northern

PAP. (2023a, December). *Chersoń: Ukraińców torturowano każąc im uczyć się prorosyjskich wierszy*. *Rzeczpospolita*. https://www.rp.pl/konflikty-zbrojne/art38052181-cherson-ukraincow-torturowano-kazac-im-uczyc-sie-prorosyjskich-wierszy

PAP. (2023b, December). *Pracownik Elektrowni Atomowej: Rosjanie zagrażają światu, awaria elektrowni oznaczałaby katastrofę*. Polska Agencja Prasowa. https://www.pap.pl/aktualnosci/news%2C1412828%2Cpracownik-zaporoskiej-elektrowni-atomowej-rosjanie-zagrazaja-swiatu-awaria

PAP. (2024, January 18). *"Na zlecenie Rosji". 17 lat temu zmarł otruty polonem Aleksandr Litwinienko*. Polskie Radio. https://www.polskieradio.pl/39/156/Artykul/2854131

PAP. (n.d.). *Rosjanie wywożą dzieci z Ukrainy. Ukraińska RPO: indoktrynują je, aby walczyły przeciwko swojej ojczyźnie*. Polskie Radio. https://www.polskieradio.pl/399/7977/artykul/3217605

Polska Agencja Prasowa. (2023, December). *Nazistowska retoryka Kremla. Ekspertka: Artykuł w RIA Nowosti de facto postuluje eksterminację narodu Ukrainy*. Forsal.pl. https://forsal.pl/swiat/ukraina/artykuly/8397340,ria-nowosti-tekst-co-rosja-powinna-zrobic-z-ukraina-nazistowska-retoryka.html

Pospiszył, I. (2008). *Patologie społeczne*. Wydawnictwo Naukowe PWN SA.

Sommer, T. (2014). *Operacja antypolska NKWD 1937–1938: Geneza i przebieg ludobójstwa popełnionego na Polakach w ZSRR*. 3 Media Sp. z o.o.

Stankiewicz, M. (2006). Zasady odpowiedzialności zbrodniarzy wojennych przed Międzynarodowym Trybunałem Wojskowym. *Studia Prawnoustrojowe, 6*, 145–162. https://bazhum.muzhp.pl/media//files/Studia_Prawnoustrojowe/Studia_Prawnoustrojowe-r2006-t-n6-s145-162/Studia_Prawnoustrojowe-r2006-t-n6-s145-162.pdf

Stempin, A. (n.d.). *Zabójstwo Anny Politkowskiej. Czy śmierć dziennikarki była prezentem dla Putina?* Wielka Historia. https://wielkahistoria.pl/zabojstwo-anny-politkowskiej-czy-smierc-dziennikarki-byla-prezentem-urodzinowym-dla-putina/

United Nations Office of the High Commissioner for Human Rights. (2022, December). *UN report details summary executions of civilians by Russian troops in northern Ukraine*. https://www.ohchr.org/en/press-releases/2022/12/un-report-details-summary-executions-civilians-russian-troops-northern

Veterans Today. (2022, February 21). *Full text of Vladimir Putin's speech*. https://veteranstoday.com/2022/02/22/vladimir-putin-full-text-of-february-21-2022-speech/

Wilk, A. (2023). *Na Zachód patrz! Reorientacja Sił Zbrojnych Rosji na południowym kierunku strategicznym*. Ośrodek Studiów Wschodnich. https://www.osw.waw.pl/sites/default/files/komentarze_350.pdf

Wojnowski, M. (2015, October). *Mit „wojny hybrydowej". Konflikt na terenie państwa ukraińskiego w świetle rosyjskiej myśli wojskowej XIX–XXI wieku*. *Przegląd Bezpieczeństwa Wewnętrznego ABW, Specjalne wydanie „Wojna hybrydowa"*, 7–38. https://abw.gov.pl/download.php?s=18&id=3400

Wrzosek, M. (2018). *Wojny przyszłości: Doktryna, technika, operacje militarne*. Fronda PL Sp. z o.o.

Żochowski, P. (2015, October). *Rosyjska „niewypowiedziana wojna" – konsekwencje dla sektora siłowego FR*. *Przegląd Bezpieczeństwa Wewnętrznego ABW, Specjalne wydanie „Wojna hybrydowa"*, 74–84. https://abw.gov.pl/download.php?s=18&id=3400

Section 3: Improving Professional Military Education

Chapter 16: Shaping Our Future: Reflections and recommendations on professional military education at the Royal Military College of Canada

A/SLt Isaac **Nitschke**, ORCID: https://orcid.org/0009-0009-2529-7975

Abstract:
With the recent publication of Justice Louise Arbour's report that recommended such measures as inquiries into whether Canada needs the Royal Military College of Canada (RMC) as it currently exists, to a recommendation to eliminate the cadet chain of responsibility, there has been serious debate on how professional military education (PME) is to continue in Canada. PME is a cornerstone of force generation in Canada; this paper aims to identify issues with the current model. Next, this paper presents feedback and proposed solutions to the identified issues based on key considerations of PME systems, namely the balance of academic and military training. This feedback draws from combined personal experience and best practices set out in previous literature or by other military academies. Ultimately, this paper concludes by arguing that PME in Canada must restructure itself to better prepare junior officers for their careers and the contemporary geopolitical environment and should seek to alleviate ethical and misconduct issues by prioritizing education in ethics and leadership.

Keywords: Military Education, development, officers, leadership, Canada

Introduction

On May 17th, 2024, the Royal Military College of Canada (Kingston) [RMC] commissioned roughly 200 new Second Lieutenants and Acting Sub-Lieutenants into the Canadian Armed Forces [CAF] upon their completion of the Regular Officer Training Plan [ROTP]. ROTP at RMC is truly "a university with a difference," holding as degree requirements academic success, bilingualism, physical fitness, and military leadership qualifications (University Study, 2024). The class of 2024 was commissioned into a period of great geopolitical and domestic uncertainty, with ongoing conflict in Europe, the Middle East, and Africa, along with rising tensions in the Indo-Pacific and North America. On the domestic front, these young officers have taken leadership of an organization in an age of budget cuts, reconstitution, and evolution, with the Minister of National Defence going so far as to characterize the CAF as being in a "death spiral" (D'Andrea, 2024). As a 2024 graduate, I have had unique opportunities to reflect on RMC, seeing it from various perspectives, whether through interactions with cadets from academies around the world, taking on senior leadership positions at the college, or working closely and developing friendships with

members across various ranks in the CAF. This paper is built on those perspectives and my thoughts and opinions that have emerged. It is by no means a representation of the opinion of the CAF or RMC.

In light of current events and recent history, this paper will discuss the purpose of RMC in the context of recent and ongoing issues. Drawing from these, the aim is to outline recommendations and broad concepts for approaching professional military education [PME]. This endeavour involves not only assessing Canada's strategic priorities in the current geopolitical landscape but also assessing the domestic landscape from which the military is drawing in personnel and that it should rightfully represent. This will highlight key elements of the most recent defence policy update, *Our North Strong and Free*, and the *Independent External Comprehensive Review* of the CAF, henceforth the Arbour Report, and my personal experiences at the college.

Purpose of RMC and PME

"Truth, Duty, Valour," the motto of RMC, embodies, to an extent, the aims of the college and the broad purpose of PME. The motto was created by the first commandant of RMC and is an ethos by which officer cadets are to live: being honest and truthful, even when it is difficult, this includes admitting one's short-comings and faults; carrying out their duties without pause or reservation, the expectation of service before self; and, having the courage and strength of character to stand up for what is right. This ethos is words to live by for the cadets and has been translated into RMC's mission statement:

> "As a military university, the Royal Military College of Canada educates, develops, and inspires bilingual, fit, and ethical leaders who serve the Canadian Armed Forces and Canada" (Royal Military College of Canada, 2024).

This statement imbues elements of truth and valour through ethical leadership and duty through the concept of service, bilingualism, and fitness. The mission statement also outlines key characteristics of the four pillars: Academics, Athletics, Bilingualism, and Military Leadership, which are what make RMC "a university with a difference" (University Study, 2024). These four pillars are important elements to success at the college, but also broadly within the CAF.

Academics constitute successful completion of a major in either Engineering, Sciences, or Social Sciences and Humanities. The selected major is complemented by a core curriculum of social sciences and humanities, including Canadian and military history, Canadian and international politics, psychology, English (*or French*) literature, and ethics. For students in the social sciences and humanities, this includes core courses in maths and science.

The Athletics pillar was designated as successful completion of the Physical Performance Test [PPT] and the FORCE Test, which is the CAF's standard fitness test. In Fall 2024, the PPT was removed as a graduation requirement, and in February 2025, it was entirely removed. The remainder of the fitness pillar is constituted by physical education classes, which range from elements of general health and fitness, such as healthy eating and proper exercise technique, to training in specific sports, including grappling, ice hockey, swimming, and a variety of racket sports.

The bilingualism pillar is another graduation requirement at RMC. Because Canada has two official languages, it was deemed important that the only federal post-secondary institution not only offer courses in both official languages but also mandate that all students learn their second language. Successful completion of this endeavour is measured by achieving a language profile in line with Canada's public service language test.

Finally, the military pillar is threefold; it mandates the successful completion of the Basic Military Officer Qualification [BMOQ], which is required for one to attain their commission, successful completion of leadership and administrative positions within the Cadet Wing, and completion of all mandatory professional development administered at the college. The Cadet Chain of Responsibility [CCoR] is the leadership element of this pillar with leadership and administrative tasks at the section, flight (*platoon*), squadron, division, and wing levels. The goal of the CCoR is not only to facilitate the administration and discipline of the college but also to allow cadets to practice leadership. Discipline at the college thus varies between squadrons, due to different cadet and Training Wing leadership. One of the most commonly used forms of discipline is called "5s and Gs" (*the college 5s uniform, worn with parade boots, gaiters, and a pillbox*), which includes additional inspections by the CCoR. There are a few other remedial measures employed at RMC, but historically, summary hearings have also been used to discipline cadets when they violate orders and directives.

The four-pillar program and the core curriculum were developed in the 1990s, with the incidents of gross misconduct culminating in the Somalia Affair. That incident, where Canadian soldiers tortured and killed a civilian detainee in Somalia, forced the CAF to undergo massive changes, in particular re-examining RMC and PME structures. For officers, the vision was to rebuild a competent, professional, and ethical officer corps following eight initiatives. First among them, intellectual development; second, improving the common body of knowledge; third, the development of policy and doctrine; then strengthening of a military ethos; followed by cultivating external relations; improving the flexibility of officer professional development; providing organizational capacity and resources; and, establishing accountabilities, incentives, and performance management (Haire 2016, p.32). These steps were important to reform RMC's

curriculum and BMOQ; all PME in Canada now had a core of defence ethics. This core was developed by the Defence Ethics Programme, which oversees the instruction and development of material for the instruction and implementation of ethics in CAF institutions and instruction. From this program, two books: *Duty with Honour* (2003) and *Trusted to Serve* (2023), have been published. Together, they outline the ethical expectations of leaders and members of the CAF. These books and the Defence Ethics Programme enshrined new elements of RMC's core curriculum ensuring that ethics become a critical element to the completion of BMOQ and Cadet leadership (*fundamental to the Military pillar*), and creating two academic courses in leadership and ethics (*in third and fourth year respectively*), as well as further courses to give cadets context of Canadian politics, international affairs, and history. With values similar to RMC's motto and instruction in ethics, all of which are put in the context of Canadian politics and history, one might ask where the problem lies.

Problematic

Starting in 2021, the CAF lost several senior leaders in the General and Flag officers ranks, largely due to allegations and investigations into misconduct, most notably this implicated two Chiefs of the Defence Staff, Jonathan Vance and Art MacDonald, both RMC graduates (Burke & Brewster, 2021). These losses rocked the CAF and RMC to their cores and have led to a deep distrust of the military and its leadership; a distrust compounded by the current geopolitical environment.

When discussing the leadership of the CAF, eyes turned to RMC as a "cradle of leadership." This opened up past issues of mental health struggles at RMC, sexual misconduct at the college, and overall, the utility of the college in producing officers. The Arbour Report (2022) identified at least four recommendations related to RMC's leadership, training, and management, and called for an independent review of RMC's existence. The first recommendation, Recommendation 23, deals with the military staff posted to RMC in the Training Wing (Arbour 2022, p.215). These members oversee the day-to-day administration of cadets and administer instruction and professional development from a military perspective. In the past, these have often been viewed as "punishment" or "promote" postings. These postings are used to remove toxic or underperforming members from their current trade, unit, or career path, placing them somewhere they will "do the least harm" (Arbour 2022, pp. 214-5). These are detrimental to RMC's staffing, particularly as members may be disincentivized from taking on postings to training institutions because they are seen as a step-down or aside from their career path. This also has implications

for the perceived quality of leadership at the college and can be detrimental to the morale, instruction, and professional development of cadets.

Recommendation 25 discusses expedited release mechanisms for candidates undergoing probationary training, including ROTP and training at the Canadian Forces Leadership and Recruit School, who do not meet ethical and cultural expectations (Arbour 2022, p. 217). However, misconduct, or inability to conform to ethical and cultural expectations, is not always reported for various reasons. First, the CAF is hurting for members and is hoping to retain as many as possible. Second, with staffing issues, leaders and members are often overworked and do not always notice when there is an issue; on the opposite end of the spectrum, some members and leaders do not want to deal with these issues. There are also cultural implications; members may not report misconduct for fear of repercussion, and in some cases, do not know how to deal with misconduct effectively. In some cases, it is a perfect storm where all these issues compound into a failure of leadership by staff and cadets at RMC, and lead to low-quality officers falling through the cracks. These few have led to a consensus among many non-commissioned members that RMC graduates are careerist, elitist, and ego-centric micromanagers. Characteristics that are not representative of effective or good leadership, and this reputation, although not universally true, poisons the reputational power of the institution. Some of these behaviours, although not explicitly taught at RMC, are a by-product of RMC's structure and culture.

The structure and culture at RMC are developed in part by the structure of the Cadet Wing and the CCoR. Recommendation 28 calls for the dissolution of the CCoR, due to abuse of authority, immaturity, and a lack of training (Arbour 2022, p.226). While the CCoR is flawed, it is invaluable to the administration, training, and support of college activities. The CCoR is often characterized as "children leading children" because cadets have little experience in the military, and it is argued that they lack the qualifications to lead other members, particularly their peers. This often devolves to emulation of behaviour seen in their superiors or their staff on the military courses they have taken (*mostly BMOQ*), which is not necessarily conducive to long-term leadership behaviours and ties into poor staffing of training institutions. A lack of training and poor role models also emphasize issues in reporting schemes and structures. Some cadets, who undertake CCoR positions for their check-in-the-box to graduate, seldom get involved or take ownership of others, avoiding responsibilities and resorting to simply forwarding emails. Others, when in uncertain or ambiguous ethical situations, fail to realize when they are out of their depth or choose to ignore it. Not everyone is suited to leadership, although some strive for it (*for better or worse*). These cadets who lack training in how to appropriately lead go on to micromanage or mismanage their subordinates, undermining trust and confidence in the CCoR and, invariably, the

Training Wing. Subsequently, when some of these leaders are rewarded or not given feedback for their "leadership," this behaviour is reinforced and replicated after graduation. Finally, the CCoR, as a peer leadership structure, has a network of personal relationships at play. These relationships allow for the use of shortcuts, favours, and deals that can subvert the effectiveness of the CCoR or bypass inefficient individuals. This is not an uncommon issue and exists in many organizations, but the bypassing of inefficient individuals can not only create an artificial self-perception of leaders but also a normative acceptance of subverting chains of command. This can also create stovepipes, which overburden cadets or create informational chokepoints, increasing uncertainty and inefficiency and impacting stress and burnout.

The military pillar is also responsible for the oversight and discipline of cadets, which is jointly carried out by the CCoR and the Training Wing staff. There have been key issues with discipline, namely, discipline being enforced and the so-called "punishment fitting the crime." Remedial measures in the CAF follow several principles, and they are intended to inform the member of improper conduct or a performance deficiency, assist the member in correcting their deficiency, and provide time for the deficiency to be corrected (National Defence, 2007). The consistent use of "5s and Gs," essentially wearing a distinctive order of dress, is an impractical solution that does not fit in the intended spirit of remediation. 5s and Gs do not correct improper behaviour; in some cases, cadets do not understand the purpose of the punishment. Furthermore, for certain performance deficiencies, 5s and Gs do not fit the violation. What relationship exists between the uniform one wears and tardiness or submitting a leave pass incorrectly?

Finally, Recommendation 29 involves the implementation of an external review to evaluate the benefits, disadvantages, and costs of continuing to run RMC (Arbour 2022, p.234). This involves a value assessment of whether RMC is accomplishing its mission statement and producing officers of a high calibre. It is the Arbour Report's proposed mechanism for addressing the college's failures and determining whether the college's current structure is an appropriate means for the college to continue.

The findings of the Arbour Report come from wide data sources, including public and policy-maker perceptions of RMC and the CAF, which were not aided in the debacle that followed Vance and MacDonald's resignations (Burke & Brewester 2021). These perceptions are shaped by the information environment and mainstream media, which have often held a great deal of scrutiny towards the college, in many instances, reasonably so, because scrutiny is a basis of a free and democratic society. News reports on RMC often fail to account for the entry age of cadets; many enter the college around 17 years old, with some as young as 16 (*Cadets from Quebec may enter RMC at Saint-Jean-sur-Richelieu to complete the requirements of CEGEP (Collège*

d'enseignement général et professionnel) because Quebec's high school system ends earlier than the rest of Canada). Across the entire college, the average cadet age is around 21 years old. While this should not be a reason to excuse a cadet's actions, the consensus of the developmental psychology community is that the brain does not fully develop until a young adult is in their mid-20s, with adolescent years being fundamental to identity formation and development of higher executive function and reasoning (Arain et al., 2013; Cherry 2024). However, what fails to be accounted for is the age and experience of cadets coming into the college. The average cadet arriving at RMC is 17, with the average age of cadets around 21. These cadets are still developing and learning; in some instances, mistakes will be made. While cadets should be held accountable for their actions regardless of age, they must also be allowed to learn and develop beyond their worst mistakes. The failure to recognize this when judging the college has led to setbacks in the institution's learning, cadets' perceptions of the college, and recruitment into the CAF and RMC.

The geopolitical environment has important implications for national policy, including PME. Specifically with the question of what one trains for, this echoes the dilemma of the "the war - a war" debate on American military readiness level in the 1990s and 2000s. This debate begs whether one prepares for the conflict they are facing or simply any conflict. In either case, knowledge is power, and ensuring a consistent level of knowledge across the officer corps is important to producing competent leaders who can execute their missions in the context of a broader strategic environment. When Charles Krulak (1999) outlined his concept of the "three-block war," he argued the need for leaders, particularly junior leaders, who can make well-reasoned and independent tactical decisions under stress; these tactical decisions, he argues, have subsequent repercussions at the operational and strategic levels (p.16). When PME was reformed in the 1990s, this was done in the context of the planned operational environment of the 21st century (McKay et al., 2022). But that environment has since passed, and there is a re-emergence of great power competition (Eyre, 2022). In the initial reforms, an important point is made about making the pillars mutually reinforcing, which they currently are not; the notion was to bridge content from the military pillar into the academic pillar, particularly elements of military history, politics, international relations, leadership, and ethics (McKay et al., 2022). But this has faced challenges, firstly, the professional development (*military training*) occurring at RMC seldom develops on or relates to the core curriculum. The core curriculum is built on science, social science, and humanities, to meet general officer specifications, in other words, the expected capabilities of an officer (McKay et al., 2022). While this is good in theory, in practice, there are issues beyond a lack of synchronicity with the military pillar and training wing. The academic curriculum based on degrees, while important, has failed to assert the importance of the core

curriculum courses for developing and producing military officers. At the ground level, cadets see these core curriculum courses as useless or impediments to commissioning, and though they complete the requirement (*to get the check in the box*), many do not retain the material, and many do not try. This has important repercussions for an officer's situational awareness upon graduation, particularly in developing "strategic lieutenants." The current information environment must be confronted with knowledge and awareness of how easily and quickly information can be distorted and spread, including how it can harm operations and the CAF. In the context of tactical-level leadership, education and knowledge should help inform decisions made by junior leaders and can help produce better outcomes at the operational and strategic levels (Krulak, 1999, p.16). Given this, the core curriculum's importance must be stressed to cadets as it is the current geopolitical climate, information environment, and domestic political climate that will shape their careers and ultimately their decisions. Having cadets acknowledge this would not only aid in their professional development but would be beneficial to their engagement with the topics.

Another important consideration of the military pillar is both summer training, positions on courses over the summer, and maintenance of military skills developed on training, many of which make up one's Individual Battle Task Standards [IBTS]. Having an up-to-date IBTS is required for personnel to deploy or participate in operations, or to get onto specialist courses, this involves qualification on their required weapon platform; retraining on the use of chemical, biological, radiological, and nuclear protective gear; successful completion of the FORCE test; first aid and CPR re-certification; and holding an appropriate security clearance along with refamiliarization with operational security. These standards are a crucial and fundamental part of one's duties. Not only do these skills help cadets maintain or hone their IBTS, but they can also set them up for greater success on courses over their summer terms or after graduation. These skills are seldom maintained at the college, and some cadets do not renew the skills between completing BMOQ and graduation, in some cases, for four or more years. For cadets, this has undermined their feelings of serving and fulfilling their duties to Canada. This also has implications for the current state of professional development at the college. Professional development has been haphazard at the college for several years, while some of it has been relevant: learning how to do administration and paperwork, writing briefing notes and memos, or learning about postings. However, professional development has consistently lacked a plan or desired outcomes. It has also lacked tangible relevance to the military profession or trade-specific requirements. Finally, the summer training blocs have often been given a backseat to academic work or second language training. Second language training is highly valuable and should not be replaced. Several past instances have included a lack of funding for on-the-job training, which is a substitute for cadets

whose professional courses would run longer than the summer block. Failures in staff work, which go hand in hand with some of the military staff posted to RMC, have limited or increased the complexity of course loading from RMC, or entirely undermined efforts to load cadets onto specialized courses.

The Arbour Report and other literature have highlighted inadequacies in the military and academic pillars examining the CCoR and the core curriculum's lack of incorporation with the military pillar. The other pillars of the RMC programme are equally under scrutiny. The athletics pillar, as of February 2025, has effectively been discontinued. Before that, cadets were required to complete and successfully pass the Physical Performance Test [PPT] twice in their time at RMC. If unsuccessful cadets were to undertake supplemental physical training to bring them to the level at which they could pass if the cadet was unsuccessful, they would be re-pathed from RMC. While these harsh measures have faced a great deal of opposition and did not conform to the principle of universality of service, these measures held cadets to high standards of fitness. The fitness pillar is highly contentious because physical activity is attributed to significant benefits for stress, mental health, and operational readiness; however, several issues surround the impartiality of the PPT's standards and whether they preclude a member from effectively serving. While the effectiveness and utility of the PPT itself are debatable, a fitness pillar should continue to exist at RMC and hold cadets to high standards if only to help cadets develop healthy relationships with fitness, food, and substance abuse, which may serve them throughout their careers. Furthermore, the inclusion of a fitness pillar and the PPT add challenges that can be overcome through hard work, dedication, and perseverance, which are all important military values.

The bilingualism pillar is also a place where cadets must overcome adversity. Proficiency in one's second official language (*English or French*) is a graduation requirement and for many is a difficult hurdle. However, there are several hurdles to successful language training. RMC (*Kingston*) primarily operates in English, despite the nominal existence of "French weeks." When cadets arrive already speaking French or complete their training early on, they have few opportunities to practice once they complete their testing. While the impetus is on the cadet, several factors contribute to skill fade for those who have attained their profile. These include the operating language at RMC, social divides between anglophones and francophones, and a lack of francophone staff.

RMC, in the 1990s, was intended to be a beacon for the birth of a new breed of CAF officers who are ethical, knowledgeable, bilingual, and fit. The design was that these officers could flow into the forces and, by influence and quickly climbing the ranks, could generate positive institutional change (McKay et al., 2022). However, these lofty goals have fallen short, and RMC officers still

have issues with creating an ethical climate. In the way of “Professional” and “Military” education, there is little occurring at RMC, and what does occur is few and far between or gets overlooked. This is indicative of a broken system, but it draws important conclusions on the purpose of PME as a whole.

Lessons Learned and Proposed Solutions

In the last section, key issues in Canada’s current PME structure for young officers were highlighted. These issues range from leadership to academics and professional development. The issues at the forefront of this are diverse, but chief among them have to do with education. RMC and other PME institutions are intended to be a learning environment; the objective should not only be in educating officers but in providing opportunities to try and fail. This should ring true when dealing with ethics, leadership, and the core curriculum.

The first solution involves rethinking RMC’s priorities and its mission. The current mission puts little emphasis on the professional and military aspects of education, and the core curriculum has expanded and shifted, in some respects, away from military considerations. As such, the mission statement should be revised to include the drive to enable future officers to be professionally competent. Such a mission statement could be framed as follows:

> “As a military university, the Royal Military College of Canada aims to educate, enable, develop, and inspire bilingual, fit, ethical, and professional leaders who serve Canada and the Canadian Armed Forces” (Royal Military College of Canada, 2024).

With this revision in mind, the college must adapt and consider the desired outcomes of PME at RMC. Reforms should ideally be manifested as a joint venture between the military and academic pillars to refocus education by bridging the military and academic pillars, making them complement one another.

Reforming the Military Pillar

The core components of PME are the professional and military aspects. In creating a junior officer, one hopes to instil the ability to lead, discipline, respect for rules, orders, and directives, and develop professional skills and competence. These are facilitated by the CCoR, the disciplinary structures at RMC, and the delivery of professional development and academic courses.

Leadership at the college is an essential component of professional development and needs to be more than a check-in-the-box. This also means that it cannot devolve to forwarding

and writing emails, while this may be representative of the administrative side of leadership, cadets also need to learn how to engage and interact with their subordinates, as well as advocate for them. CCoR positions are an opportunity for senior cadets to inspire and teach junior cadets, augmenting the socialization process, but also an opportunity for failure and experimentation. Because of its importance, it should be afforded greater resources, training, and opportunities. In terms of training, candidates selected for CCoR positions need adequate prerequisite training. Currently, this means completion of BMOQ; however, there should be more. Cadets taking on CCoR positions should be required to learn administrative procedures and policies, as well as how they can best support subordinate cadets. This would not only involve giving cadet leaders, at more junior levels, greater responsibility, but also greater ability to mentor subordinates and receive mentorship. This educates cadets on the process of administering their subordinates and enabling them to help or facilitate the administration of others, which is a critical task for junior officers. The administrative apparatus and oversight should also be expanded to include performance appraisals of junior/subordinate cadets and all CCoR positions. These could be done following the current performance evaluation and review [PER] system in place in the CAF, although on a smaller scale. Using PER-like evaluations would not only streamline the performance appraisal process but also serve as a tool to identify deficiencies; furthermore, it would enable the Training Wing to have better oversight of a cadet's deficiencies and prospects for more senior leadership positions. This system would be a way for cadets to get feedback on their leadership and accomplishments, and this task could be rolled into the present third-year "leadership" course, *Organizational Behaviour and Leadership*, as a practical requirement. The leadership aspect of the military pillar should be further reformed to incorporate mentorship. While presently senior CCoR appointments receive mentorship from their counterparts in the Training Wing, the junior positions receive minimal supervision or mentorship. Incorporating mentorship of subordinates through a PER system and as a component of an academic course can create more accountability and develop better leaders by giving them opportunities and feedback on their progress.

Discipline is a cornerstone of the military, leadership, and PME. RMC's current model instils little familiarity with the disciplinary and remedial mechanisms of the CAF, or with an effective understanding of how to carry out remediation. There are two primary mechanisms at the lowest levels: summary hearings and remedial measures. Summary hearings are a non-penal method to address minor breaches of military bearing at the unit level fairly and quickly, they deal with minor service infractions related to property and information, breaches of military discipline, and use or possession of alcohol or cannabis (*legal under Canadian law*) on duty (National Defence, 2024).

While remedial measures deal with performance, they are specifically a tool to assist members in overcoming their performance deficiencies (National Defence, 2007). A PER system can be used to facilitate remediation. Updates can be made on a subordinate's file, along with a plan for how they can correct their deficiency, followed by a monitoring period. This is a more effective and practical means to remediate; furthermore, it aligns better with a leader's responsibilities in the CAF. Ideally, this method would do away with 5s and Gs and adopt a more pragmatic approach where the measures have a link to the deficiency. Such a framework could be done in a way that has little impact on a cadet's prospects at the college, save for extreme measures that constitute a service violation or that are beyond the scope of an RMC cadet's purview. This would require additional training for cadets in the CCoR to understand their limits, their ranges, and their responsibilities in this mechanism. It would not only facilitate solving problems at the "lowest" level but also allow the CCoR to pass deficiencies and misconduct up the chain for review. For major deficiencies or violations of protocol, the incorporation of summary hearings is a public format that helps dispense discipline to cadets. The public element of summary hearings acts as both a deterrent and a means to demonstrate that violations of order and discipline will not be tolerated. This mechanism would develop cadets professionally and instil in them a better understanding of CAF remedial measures and structures.

Professional competence is an important skill to develop at RMC. This is embodied both by the IBTS and through professional development [PD] within and outside of the college. Continuity of PD and keeping the "military" in PME is a motivation for cadets, allowing them to feel they are contributing to the CAF's mission. Maintenance of cadets' IBTS is a small part of this. Organizing ranges, CBRN training, and renewing first aid courses are a small part of this process. Practical military training and PD should be prioritized by leveraging the expertise across the training wing at the college. This can include changing how PD is delivered, which should involve splitting up cadets not only by academic year but sometimes by trade and/or environment. If one centralizes all services into one academy, there needs to be a way to offer distinctive and crucial training for each cadet, and meaningful training should have a rapport with their future occupation. Academics can support such an endeavour, help support and develop what is taught or discussed in PD, establishing links with specific occupational or operational challenges, and explaining how situations on the blackboard translate to the battlefield. Developing a strong PD program involves getting buy-in from the cadets and all wings of the college, as well as allocating sufficient funding to give cadets opportunities to undertake relevant on-the-job training or courses over summer. This involves coordination at the highest and lowest levels within and outside the college to prioritize summer courses, or at a minimum, allocate several spots for cadets from RMC.

In developing or reforming a PME structure, the professional and military components must be taken seriously. These elements are to be complemented by the broadness and open-mindedness of education but are also a sandbox where cadets may practice their leadership and learn how to administer members in a large organization like the CAF. PME is enhanced by offering leadership opportunities and giving the appropriate training and feedback to cadets in these positions. It is also supported by a disciplinary system that allows for mistakes to be made and supports cadets as they work to overcome their deficiencies. Finally, PME is strengthened when one promotes military training and supports it with academic perspectives. Ultimately, these concepts together help to develop officers who are more familiar with the organization and procedures, strengthening the CAF's leadership.

Educating an Officer: Ethics

The instruction of ethics must be approached cumulatively. Ethical behaviour is not something that happens overnight but is rather an ongoing socialization process that is communicated and developed implicitly and explicitly (Little, 2016). If one is seeking to bring about real ethical change, then one must be willing to take small steps to produce incremental change. The first step should be taken early in a cadet's career to arm cadets with a language and frameworks through which to understand and apply ethics; this would build a common and robust ethical framework which is both top-down and bottom-up. This is exemplified at the United States Naval Academy through their ethics and leadership education which starts in their preliminary training (*Plebe Summer, which is arguably not the best name*) and continues through all their years, culminating in a course*: Law for the Junior Officer*, which condenses the US Military Code of Justice, the Law of Armed Conflict, and maritime law into a single course (United States Naval Academy n.d.). Unlike RMC, which condenses military ethics, leadership, and law into a single semester-long course, the US takes a long-term socialization approach to the development of ethical leaders. While it may be imperfect and may come at the expense of academics, it is an elegant solution to the problem at hand. RMC approaches these topics both through professional development and academic courses, but the first academic course where ethics is approached is a third-year course, *Organizational Behaviour and Leadership, and it focuses more on basic psychology*. It is perhaps better to install an additional, or supplement, a first-year course, creating an "*Introduction to Ethics and Moral Reasoning*." The objective is to instil cadets with language and frameworks through which they can understand and communicate ethical issues and dilemmas. This would help instigate a broader socialization process, allowing cadets to grow their

knowledge and experience with the topic over time, learning and growing from further exposure and awareness of ethics and their importance.

Educating an Officer: The Political Context

PME structures do not exist in a vacuum and depend on the broader political context. Presently, RMC's core curriculum is designed to bridge knowledge gaps as to Canada's domestic and international political approaches and Canada's historical role. By reinforcing ethical education, RMC can better approach Canada's domestic political climate and demands, but the military pillar must collaborate when approaching the geopolitical elements.

Military education, particularly one that adopts a university format, must operate in the context of domestic society and be a roughly accurate representation of society (*this will almost always be imperfect*). RMC must maintain public confidence both through preparing cadets to serve Canada and instilling them with the strong moral leadership qualities that Canadians want to embody. This also means that RMC must embody national values, which for Canada include diversity and multiculturalism. This is one reason for some of the core curriculum courses but should also be accomplished through general socialization. Cadets should not be cut off from society and should have avenues to interact with members of the public as CAF members. Through conferences, events, and outreach activities, cadets can be doubly socialized in a military environment and in a civilian setting, where they do not lose touch with the people they serve. Ideally, this should serve as a moderating effect on military socialization and would create more well-rounded officers who better embody public interests.

From a geopolitical standpoint, PME should be delivered in the context of current geopolitics and history. When developing a PME structure, there must be simultaneous preparation for "the" war and "a" war. By preparing for "the" war, cadets are prepared for the geopolitical environment they will commission into with an understanding of current tensions and operations that they will likely take part in. When cadets graduate, within one to two years, they may wind up deployed on a named operation, in a time of heightened conflict. With this in mind, cadets must be prepared for the world they will operate in when they graduate. However, cadets must also be for "a" war. This is facilitated through education on history and military practices, the idea being that cadets are prepared for any conflict they face throughout their career (*which is hopefully a long one*). These contexts will differ over time and mean that professional development delivered for the military pillar, and augmented by the academic pillar, must be adaptable to suit the current demands. This means that course and PD content should be relevant to educating cadets about ongoing operations and conflict, considerations and decision-making (*ideally across*

levels). Where military lecturers and faculty can help deliver the military considerations, academic faculty can contextualize ongoing issues and military decisions with academic backgrounds. If this content shifts along with national strategy and policy, cadets are more likely to be familiarized with the current environment and with ongoing changes and evolution.

Presently, the world is seeing threats to the rules-based international order and the re-emergence of great power competition, which is exacerbated by threats to sovereignty, global instability, and rapidly advancing technology (National Defence, 2024a). *Our North, Strong and Free* discusses these issues, and Canada's defence policy should be incorporated into the delivery of RMC's content. Professional development should incorporate and discuss key themes like Arctic sovereignty, defence procurement, recruitment, retention, and culture change. Cadets must leave the college with a degree of familiarity with the CAF's role in the world and its strategic outlook. Examining defence policies, both professionally and academically, will allow cadets to understand the vision of the CAF and the changes that will come in the short and medium term and will impact their careers. This will also affect how cadets perceive their duties and give a perspective that informs their decision-making at the junior and senior ranks. Finally, it will help contextualize the salience of both *academic* and *military* education to their service.

Conclusion

This chapter has contextualized the key elements of PME by exploring how RMC has come under scrutiny through the *Arbour Report*. By taking the report's recommendations and incorporating the geopolitical environment, it proposes ways forward for RMC and other PME institutions that seek to follow the Canadian model. The chapter has found that PME systems are a fine-tuned structure that requires a balance between disparate elements and often demands a holistic effort and coordination to be successful. To maintain academic credibility and legitimacy, there must be high-level academics who not only complement military training but that develop knowledge and understanding beyond military confines. Equally, the structures of PME institutions must echo their parent organization, ensuring discipline and effective professional development for future integration into the organization. Finally, the military and academic training must not be removed from the contexts of the domestic and international political settings, after all the military is subordinate to the government of the people in a democratic setting. This emphasizes the importance of developing officers who uphold the morals and values of society and who are prepared for not only the current geopolitical environment but also potential future conflicts.

References

Arain, M., Haque, M., Johal, L., Mathur, P., Nel, W., Rais, A., Sandhu, R., & Sharma, S. (2013, April 3). “Maturation of the adolescent brain.” *Neuropsychiatric Disease and Treatment*, 449-461. https://doi: 10.2147/NDT.S39776.

Arbour, L. (2022). Report of the Independent External Comprehensive Review. In *Canada.ca*. Department of National Defence. https://www.canada.ca/en/department-national-defence/corporate/reports-publications/report-of-the-independent-external-comprehensive-review.html

Burke, A., & Brewster, M. (2021, October 21). A military in crisis: Here are the senior leaders embroiled in sexual misconduct cases. *CBC*. https://www.cbc.ca/news/politics/sexual-misconduct-military-senior-leaders-dnd-caf-1.6218683

Cherry, K. (2024, July 29). *Understanding Developmental Psychology: Physical, Cognitive, Emotional, and Social Development Through the Lifespan*. https://www.verywellmind.com/developmental-psychology-4157180.

D’Andrea, A. (2024, March 7). Canada’s military facing ‘death spiral’ on recruitment, minister says. *Global News*. https://globalnews.ca/news/10341588/canadian-forces-recruitment-death-spiral/

DAOD 5019-4, Remedial Measures, 4 (2007). https://www.canada.ca/en/department-national-defence/corporate/policies-standards/defence-administrative-orders-directives/5000-series/5019/5019-4-remedial-measures.html#gp

Eyre, W. (2022, November 2). U.S.-Canada Defense Partnership in a Dangerous World [Interview]. In *CSIS Events*. https://www.csis.org/events/us-canada-defense-partnership-dangerous-world

Haire, K. F. (2016). *Professionalism in the Army: from Murder in Somalia to Disgrace in Afghanistan, How Far Has the Army Come?* [Thesis]. Canadian Forces College.

Krulak, C. C. (1999). *The Strategic Corporal: Leadership in the Three Block War*. Defense Technical Information Center. https://doi.org/10.21236/ada399413

Little, W. (2016). Chapter 5. Socialization. In *Introduction to Sociology - 1st Canadian Edition*. BCcampus Open Education.

McKay, J. R., Breede, H. C., Dizboni, A., & Jolicoeur, P. (2022). Developing Strategic Lieutenants in the Canadian Army. *The US Army War College Quarterly: Parameters*, *52*(1), 135–148. https://doi.org/10.55540/0031-1723.3134

National Defence. (2024a). Our North, Strong and Free: A Renewed Vision for Canada’s Defence. In *Reports and Publications*. Department of National Defence. https://www.canada.ca/en/department-national-defence/corporate/reports-publications/north-strong-free-2024.html

National Defence. (2024b). *The Canadian Military Justice System*. Canada.Ca. https://www.canada.ca/en/department-national-defence/corporate/reports-publications/military-law/judge-advocate-general-annual-report-2022-2023/ch2-canadian-mj-system.html

Royal Military College of Canada. (2024, November 18). *The RMC Mission*. RMC-CMR.Ca. https://www.rmc-cmr.ca/en/college-commandants-office/rmcc-mission

United States Naval Academy. (n.d.). *USNA Core Curriculum*. USNA.Edu. Retrieved March 3, 2025, from https://www.usna.edu/Academics/Majors-and-Courses/Course-Requirements-Core.php

University Study. (2024, October 21). *Royal Military College of Canada*. University Study. https://universitystudy.ca/school/316/

Chapter 17: Addressing the Digital Deficit in Professional Military Education

Dr. Christopher **Morris**, ORCID: https://orcid.org/0000-0002-6690-6839
Dr. Veronika **Hinman**, ORCID: https://orcid.org/0000-0002-7075-5316

Abstract:
Digital technology now permeates military environments and is integral to organisational effectiveness. However, declining digital literacy among the general population and increasing competition for specialised technology roles present significant challenges for military institutions. This chapter examines these challenges from an educational perspective, exploring how digital competencies are integrated into professional military education (PME) within the UK. It analyses current doctrine and educational practices, highlighting the limitations of traditional PME structures in addressing the growing digital deficit. The chapter argues for a reconceptualisation of PME as an experimental space for digital innovation, where emerging technologies and pedagogical approaches can be tested and refined. Key barriers to digital transformation, including institutional inertia and policy constraints, are discussed alongside potential solutions, such as interdisciplinary collaboration, scenario-based training, and civil-military partnerships. The chapter concludes that integrating digital competencies into PME is not only essential for enhancing individual proficiency but also crucial for maintaining strategic and operational effectiveness in modern warfare.

Key words: professional military education, digital literacy, cyber security, military training

Introduction

The convergence of advanced digital technologies and traditional warfare has fundamentally altered the operational landscape faced by modern militaries. As military establishments globally grapple with increasingly sophisticated cyber threats and information-driven warfare capabilities, the imperative for digitally competent military personnel has reached unprecedented levels. This technological revolution necessitates a corresponding evolution in Professional Military Education (PME) frameworks. This paper argues that PME must undergo a fundamental transformation by embracing its role as an experimental space where digital literacy and innovative pedagogical techniques can be integrated into military training. In doing so, PME can become a hub for innovative learning, equipping military personnel with the digital skills needed to meet the demands of modern warfare.

Examples used in this chapter were selected based on their relevance to digital competency development in PME and their presence in published literature or institutional reporting. The examples highlight systemic challenges or innovations, with an emphasis on

transferable lessons. Sources include defence policy documents, academic publications, and institutional case reports from both UK and NATO contexts.

The Importance of Digital Literacy in Contemporary Warfare

The Digital Revolution and Military Effectiveness

Digital technology has saturated almost every aspect of military operations, from command-and-control systems to intelligence gathering and cyber defence (Gilli et al., 2025). Modern warfare now relies on the rapid processing of vast quantities of data, real-time communication across global networks, and the ability to counter sophisticated cyber threats (Chromyszak et al., 2022). As such, digital literacy is no longer a requirement just for specialists; it has become an essential competence for all military personnel (Sangwan & Raj, 2021; Singer & Johnson, 2022). In this new era, success on the battlefield often depends on the ability to effectively use digital tools and technologies (Thiele, 2021).

Alongside advances in technology, it is digital networks that facilitate quicker decision-making, enable remote surveillance and reconnaissance, and support the integration of unmanned systems into operational theatres (Davis & Force, 2021). The military's capacity to process and interpret digital information can mean the difference between victory and defeat, with some even going as far as to conceptualise information as an emerging domain of warfare (Davis & Force, 2021). Consequently, the integration of digital skills into military training is critical not only for maintaining technological superiority but also for ensuring the overall effectiveness and adaptability of armed forces in a rapidly evolving strategic environment.

Defining Digital Literacy in a Military Context

Digital literacy has been conceptualised in several ways, with the term being used to describe the minimum skill set required to engage with life in a post-industrial society (Lankshear & Knobel, 2011, p. 52) or simply the ability to draw on digital sources, a key component of the digital age (Gilster, 1997, p. 2). The idea of digital literacy changes as technology advances (Dobson & Willinsky, 2009, p. 287; Martin, 2008, pp. 156–157), and its meaning can naturally vary between societies and industries.

Digital literacy in the military context is naturally an evolving concept, but already clearly extends beyond basic computer skills; it encompasses the ability to understand, interpret, and effectively utilise digital information and technologies in operational settings. This includes competencies in cybersecurity, data analytics, artificial intelligence, and information warfare. It also

requires an understanding of the underlying technologies that drive these capabilities, as well as the strategic implications of their use (Barron & Rowles, 2021). Along with a range of technical skills, practitioners require cognitive abilities, such as critical thinking and problem-solving to be considered digitally literate (Erbschloe, 2017).

Demand for digital skills is set to rise sharply in military occupations, with a growing emphasis on information systems and cyberwarfare compounding existing shortages in critical skills (Geluk et al., 2020). There is a clear need to identify and train a range of specialists to contend with the changing character of war, with occupations ranging from cyber operators to data experts needing to be recruited and retained (Sõmer et al., 2019; Zdzikot, 2021). The United Kingdom (UK), like many other states, can address specific roles by targeted recruitment and partnerships with industry to alleviate the worst of the shortfall (Ministry of Defence, 2025). Yet demand for digital literacy extends beyond specialists operating directly in cyber and information warfare related roles and national security requires comprehensive engagement across the population (Ivan et al., 2021). In the military context, it is vital that the whole force is engaged with the issue of cyber security (Berndtsson, 2024, p. 151; Devanny et al., 2021, p. 19).

Note that digital literacy does not refer to the capacity for an individual to succeed in a specific technology related role. Rather it is the base level of knowledge that everyone must possess in order to function at an effective level (Martin & Grudziecki, 2006). Engaging with the challenge of digital literacy in the military does not necessarily mean recruiting and training individuals for specialist roles but instead ensuring that everyone can function effectively in the increasingly digital and technologically demanding battlefield. Across the whole force, military personnel must be equipped not only to operate digital systems but also to innovate and adapt these systems to meet the demands of modern conflict. This means that digital literacy requires a shift from a static, knowledge-based curriculum to one that fosters continuous learning and critical engagement with emerging technologies.

The Growing Digital Deficit and Its Implications

Despite the strategic importance of digital literacy, there is mounting evidence of a significant digital deficit within many armed forces, including those of the UK. While specialised roles such as cyber operators have received increased attention, the broader force remains under-equipped in terms of digital competencies (Walrond, 2024). This shortfall not only hampers operational effectiveness but also undermines the military's ability to innovate and adapt to emerging threats.

Firstly, the overall picture of the UK is grim. Even outside the military, businesses struggle to secure digital talent (Lewis et al., 2024, pp. 2–3), with the skill shortage being significant enough to damage both the tech sector and the wider economy (Morgan McKinley Insights, 2025, p. 96). The issue is compounded by a lack of access to digital training and the UK's rising inequality, which both limit skills (Cole, 2017). Moreover, whilst younger generations may constitute digital natives (Dascalu et al., 2024; Ford & Vignare, 2015) who have grown up surrounded by information technology, this does not necessarily translate into useful capabilities. This all limits the UK's ability to develop its digital-industrial capabilities and creates intense competition for the restricted number of digitally skilled military recruits.

Reports from institutions like the National Audit Office (Morse, 2018; Reforming the Civilian Workforce - NAO Report, 2019) have highlighted persistent challenges in recruiting and retaining personnel with advanced digital skills. Factors contributing to this deficit include generational shifts, inadequate training infrastructures, and the rapid pace of technological change.

This can be demonstrated by the now-infamous Stuxnet cyberattack on Iran's nuclear facilities. A USB stick was inserted into the facility, enabling the cyberattack and disrupting Iran's nuclear programme (Datta & Acton, 2023). Whilst this was a unique case, it illustrates how a single individual without sufficient training can have a significant impact. In the modern era, with vast digital infrastructure, a lack of digital competency can affect national security.

So far engagement with the issue usually takes place in the context of compulsory training, often delivered through online learning packages or briefings. Whilst these are vital in terms of generating awareness and building competence with IT systems, they are also recognised as inadequate, with more advanced solutions needed to ensure effectiveness (Onduto et al., 2021; Sawyer & Emmett, 2021; Steingartner et al., 2021). Multiple delivery methods improving outcomes (Alkhazi et al., 2022). Integrating digital literacy outcomes into military academic programmes could enhance outcomes. Yet, currently, PME plays only a limited role in closing the digital literacy gap.

Limitations of Traditional Professional Military Education

UK PME Infrastructure

The British Army has its own training institutions, staffed with in-house academics, and academic subjects are taught across three departments, the Department of Defence and International Affairs, the Department of War Studies, and the Department of Communications and Behavioural Science. These departments help integrate contemporary research in leadership,

military strategy, history, and international relations into military education, ensuring that soldiers are equipped with both traditional military values and modern strategic insights (Jacobs, 2016).

The Royal Navy and the Royal Air Force have embraced external academic collaborations. Britannia Royal Naval College and the RAF College Cranwell are currently partnered with universities, the University of Lincoln (University of Lincoln, n.d.) and the University of Portsmouth, respectively. For example, the Portsmouth Military Education team provides critical analysis and research expertise in international security, air power, military theory, joint operations, space and cyber, and military history, international relations, air power, contemporary security operations and challenges, which is incorporated into the PME curriculum (University of Portsmouth, n.d.).

Complementing these branch-specific efforts is the joint PME environment facilitated by the Defence Academy of the United Kingdom. This institution serves as a central hub for inter-service education and maintains ties with external academic providers such as King's College London and Cranfield University. These partnerships enhance courses with advanced theories and empirical research on modern conflict. Thus, the Defence Academy ensures that military leaders develop a well-rounded understanding of global security, preparing them for the demands of the operating environment (King's College London, n.d.).

In short, the UK's PME landscape is characterised by a blend of in-house military expertise and dynamic external academic collaborations. These external partners operate independently of military structures and bureaucracies, allowing them to deliver tailored, cutting-edge research and education that directly addresses the needs of their military clients. Their agility and academic freedom enable them to provide critical insights on emerging security challenges, if that is what they are asked to provide.

The Historical Emphasis in PME and Its Shortcomings

At the moment, PME programmes are generally unambitious in scope. Traditionally, PME has focused on the study of past conflicts, leadership theories, and international relations, which have long served as the foundation for military strategy and doctrine (Fisher, 2022; Libel, 2021). This focus on historical case studies has played a crucial role in shaping the strategic mindset of military leaders. By examining the successes and failures of previous wars, officers have gained valuable insights into the principles of leadership, the importance of innovation, and the dynamics of international politics. Whilst these lessons remain important from the standpoint of collective identity, they are increasingly inadequate in addressing the multifaceted challenges of modern warfare.

The reliance on historical paradigms in PME has resulted in systems that are often slow to adapt to new realities. In the UK, educators continue to emphasise lessons drawn from conventional conflicts (Maguire, 2021), even as the character of warfare undergoes a profound transformation in the digital age. This emphasis on history and tradition, while fostering continuity and institutional identity, also risks creating an intellectual environment that is overly conservative and resistant to change. When historical examples are used as the primary basis for teaching, there is little room for exploring innovative approaches that address contemporary digital challenges. As a result, military personnel may be well-versed in the theories of past conflicts but lack the practical skills and critical thinking abilities necessary to confront the uncertainties of modern warfare.

Bureaucratic Inertia and Resistance to Change

Another significant barrier to digital innovation within PME is the bureaucratic inertia that pervades military institutions. The highly formalised and standardised nature of military education, designed to ensure consistency and reliability, often stifles creativity and limits the scope for experiential learning (Hasselbladh & Ydén, 2020). Bureaucratic procedures, while necessary for maintaining order and discipline, can impede the rapid integration of new technologies and pedagogical methods. This rigidity is compounded by the entrenched cultural attitudes within military organisations, where traditional methods and historical precedents are deeply valued (Soeters et al., 2007). The result is an institutional environment that is resistant to change and slow to respond to the evolving demands of digital warfare.

This resistance is further reinforced by the perception that digital skills are a niche area, relevant only to specialists such as cyber operators or data analysts. Senior leaders, accustomed to the established paradigms of military training, may underestimate the importance of digital literacy for the broader force (Farina, 2022). These attitudes lead to a persistent gap between the operational needs of modern warfare and the capabilities imparted by traditional PME. The reluctance to overhaul instruction and invest in digital infrastructure not only hinders the development of critical competencies but also undermines the military's strategic adaptability in an increasingly complex digital environment.

The Impact of Traditional Approaches on Operational Readiness

The limitations of traditional PME are not confined to academic theory; they have tangible implications for operational readiness. In today's battlefield, where digital systems and cyber operations play a decisive role (Ministry of Defence, 2022), the absence of comprehensive digital

training can compromise the effectiveness of military operations (Crilly, 2023). The failure to integrate digital skills into PME means that many officers and non-commissioned officers [NCOs] are unprepared to utilise emerging technologies. This knowledge gap can lead to delays in decision-making, vulnerabilities in cyber defence, and a general lack of preparedness for the demands of contemporary conflict.

Modern conflicts increasingly involve hybrid threats that combine conventional military operations with cyber-attacks, disinformation campaigns, and electronic warfare. Therefore, the need for a digitally proficient force is critical. Without the skills to interpret and counter digital threats, military operations risk being compromised at every level. Yet, traditional PME lags behind the realities of modern warfare. Therefore, this gap, if not critical vulnerability, must be addressed if armed forces are to maintain their strategic edge.

Reconceptualising PME as an Experimental Space for Digital Innovation

Rationale for Transforming PME

In light of the growing digital deficit and the limitations of traditional PME, military education must be reimagined. Instead of solely focusing on history and doctrine, PME must be transformed into an experimental space dedicated to digital innovation. This paradigm shift is based on the recognition that the challenges of modern warfare require a fundamentally different approach to education, one that is agile, adaptive, and forward-thinking. While institutional inertia remains a challenge, there is clear momentum for change.

The concept of an experimental PME is grounded in the idea that military education should be a dynamic, continuously evolving process (Misra, 2008). In an environment characterised by rapid technological advancements and shifting operational realities, the ability to experiment with new teaching methods and digital tools is essential. By embracing a culture of experimentation, PME can become a testing ground for innovative approaches to digital training, allowing military educators to pilot new learning strategies, assess their effectiveness, and refine their approaches over time (Boladian et al., 2024). This experimental approach not only addresses the immediate need for digital literacy but also fosters a culture of continuous learning and adaptation, both of which are crucial for long-term strategic success.

Transforming PME into an experimental space marks a break from traditional models of military education. It requires a shift in mindset, from one that is rooted in the past to one that is focused on future challenges. This transition involves rethinking the foundations of military training and embedding digital competencies as a core component. Ultimately, the goal is to create an

educational environment that not only responds to emerging threats but also proactively develops the skills needed for digital warfare.

This reconceptualisation aligns with trends seen in other NATO-aligned PME institutions. For instance, the Korea Military Academy has partnered with tech companies to deploy AI-powered simulation platforms for scenario-based learning (Altair, 2025). Such international examples demonstrate that the transformation of PME into an experimental environment is not only viable but already underway in peer systems, offering valuable models for adaptation and innovation.

Integrating Digital Competencies into the Curriculum

Achieving the vision of an experimental PME requires a structured and deliberate approach to integrating digital competencies at all levels of military education. Rather than treating digital literacy as a standalone subject, it should be embedded throughout the curriculum. In practice, this means that courses on leadership, strategy, and international relations must be complemented by modules that address the practical applications of digital technology in military operations.

A key element of this integration is experiential learning. Digital skills are best acquired through hands-on experience with technology (Mullen et al., 2019), and PME must therefore incorporate simulated environments that replicate real-world digital challenges. For example, advanced simulation platforms can provide military personnel with the opportunity to engage in cyber warfare exercises, data analysis scenarios, and decision-making processes that rely on digital tools (Brescia, n.d.). These exercises help bridge the gap between theoretical knowledge and operational application, ensuring that personnel can apply digital competencies in real-world scenarios.

To remain at the cutting edge of digital education, PME must also leverage strategic partnerships. Collaborations with technology firms, academic institutions, and organisations such as the National Cyber Security Centre can provide access to the latest developments in cybersecurity, data analytics, and digital warfare.

Finally, digital competency training must be interdisciplinary, encouraging the blending of technical skills with strategic thinking. Military personnel should not only learn how to operate digital systems but also develop an understanding of how digital technology shapes military strategy and international security. This requires a holistic approach to education, one that integrates insights from fields such as information science, cyber security, and data analytics with traditional military studies. Through such interdisciplinary training, military personnel will develop a more nuanced understanding of how digital technology can be leveraged to achieve strategic objectives.

Scenario-Based Training and Simulated Learning Environments

One of the most promising methods for integrating digital competencies into PME is the use of scenario-based training and simulated learning environments (Bagiati et al., 2024). These approaches enable military personnel to engage in realistic, immersive exercises that replicate the challenges of modern warfare.

By simulating cyber-attacks, data breaches, and other digital threats, such training provides a controlled environment for personnel to develop and refine critical digital skills without operational risks (Yamin et al., 2021). The experiential nature of these exercises ensures that the military personnel are not merely passive recipients of theoretical knowledge, but active participants in the learning process. Research suggests that experiential learning enhances retention and decision-making under pressure (Chow et al., 2011).

Empirical studies support these claims. For instance, a meta-analysis by Chernikova et al., (2020) found that simulation-based learning significantly improves performance outcomes in higher education, particularly in domains requiring critical decision-making under uncertainty. An example from outside the education sector can be found in the aviation industry, where precision and rapid decision-making are critical. Delta Air Lines implemented flight simulations that replicated a range of weather conditions and emergency scenarios. This approach led to a substantial reduction in accidents and a marked improvement in pilot competency, demonstrating the effectiveness of simulated learning environments (MDA Training, 2023).

Unlike with traditional classroom-based instruction, scenario-based training ensures that military personnel actively engage with problem-solving tasks rather than passively absorbing theoretical knowledge. As digital threats continue to evolve, incorporating such training into PME is essential for preparing military personnel to navigate the complexities of modern conflict.

Simulated learning environments offer several advantages over traditional classroom instruction. They provide interactive interfaces that facilitate immersion, allow learners to engage with complex scenarios using a combination of software and hardware, and offer immediate feedback to support learning. By enabling users to adjust aspects of reality, such as addressing rare events or shortening response times, these simulations create dynamic opportunities for practice and skill development. This has positive effects on learning and achievement (Chernikova et al., 2020).

These advantages make simulations especially valuable in preparing for the dynamic and unpredictable nature of digital warfare, where quick decision-making and adaptability are crucial. Moreover, they can be tailored to reflect the unique challenges faced by different branches of the armed forces, ensuring that training remains practical, relevant, and mission-focused.

However, expanding the use of simulation platforms requires substantial investment in technology and infrastructure. Yet, the already mentioned benefits like enhanced operational readiness, improved decision-making, and greater strategic agility, make this a necessary step. As digital technology advances, PME must therefore stay ahead by integrating these tools into its training framework. There is clear momentum for such changes. In March 2025, the UK Prime Minister reaffirmed a commitment to modernising institutions and strengthening national security, stating that 'the digital revolution underpins moves to a more agile, effective, and active state' (Prime Minister's Office, 2025). PME has a key role to play in this broader effort by equipping personnel with the skills needed to navigate an increasingly complex global landscape. Through experimentation and innovation, PME can remain agile, adaptable, and prepared for the demands of future conflicts.

Policy Barriers to Digital Transformation

Strategic Policy Reforms and Resource Reallocation

Despite some recent positive developments as highlighted in the previous section, policy barriers remain, and to overcome the barriers to digital transformation in PME, comprehensive strategic policy reforms are required.

At the highest levels, defence policy must explicitly recognise digital literacy as a core strategic objective. Policy documents such as the Integrated Operating Concept (UK Ministry of Defence, 2021), do not explicitly prioritise digital literacy and should be updated to reflect its strategic importance. This top-down approach is essential for aligning educational objectives with broader strategic imperatives, ensuring that investments in digital training are prioritised at all levels of military education.

In addition to policy reforms, significant resources must be reallocated to support the integration of digital competencies into PME. This includes investments in digital infrastructure, training platforms, and the recruitment of faculty with expertise in technology and cyber security.

Current evidence suggests that many academics teaching in the field of cybersecurity either have limited practical experience or lack a strong academic background in cyber strategy (Borghard et al., 2021). Therefore, institutional reform must prioritise the training and professional development of educators within PME. As faculty members play a crucial role in shaping the curriculum, they must themselves be proficient in digital technologies. Professional development programs that focus on digital literacy, innovative teaching methods, and interdisciplinary collaboration are essential for ensuring that educators are equipped to lead the transformation of

PME. Ultimately, resource reallocation should not be seen as a departure from traditional military training but as a necessary adaptation to the demands of modern warfare.

The Role of Civil-Military Collaboration in Driving Change

The challenges associated with transforming PME into an experimental space for digital innovation cannot be addressed by military institutions alone. Civil-military collaboration is critical to achieving the necessary reforms. As this chapter has pointed out, partnerships with civilian academic institutions play a vital role in integrating digital skills into military education, though some challenges remain. In the UK, the MoD already has partnerships with various technology companies as part of its Science and Technology Strategy, working with both industry and academia to advance innovation (Sugden, 2023).

Civil-military cooperation offers numerous benefits, fostering innovation and technological advancements that contribute to a stronger and more resilient future. These initiatives focus on areas such as force protection and mobility, intelligence, secure communications, cyber capabilities, and the integration of artificial intelligence and virtual reality, among others (del Castillo Sancho, 2023).

Beyond collaboration with technology companies, research organisations, and academic institutions, there is also a need for direct investment in digital training. In this way, civil-military partnerships serve as a catalyst for change, driving the digital transformation of PME. The innovation-driven civilian sector provides diverse perspectives and expertise, supports shared training programmes, and contributes to the co-creation of new digital tools that enhance the overall effectiveness of PME.

Conclusion

This chapter has argued for transforming PME into an experimental space that embraces digital innovation. By reconceptualising PME as a dynamic environment for testing new learning methods, it can address the current digital deficit and equip military personnel with the skills needed to navigate the challenges of the 21st century.

In the UK, PME has traditionally focused on international relations, history, and doctrine, as reflected in the Armed Forces' contracts with academic institutions. While these partnerships bring many benefits and provide valuable expertise, they only partially prepare personnel for the evolving challenges of the 21st century. Digital deficit, as one of the most pressing issues, remains largely unaddressed. PME providers in the UK and beyond must actively engage with this challenge.

However, this transformation is not without obstacles. As this chapter has highlighted, institutional inertia and entrenched cultural attitudes pose significant barriers to change. Overcoming these requires comprehensive strategic policy reforms, the reallocation of resources towards digital infrastructure and training, and a concerted effort to foster civil-military collaboration. Senior military leaders must be willing to challenge traditional paradigms and prioritise digital literacy as a core element of operational effectiveness. Ultimately, military institutions must become more demanding customers, expecting more from their academic partners.

The proposed reformation of PME is not merely an educational upgrade but a strategic necessity. A digitally proficient military force is essential for maintaining national security, ensuring operational readiness, and securing a competitive advantage in an era of rapid technological change. As the character of warfare continues to evolve, so too must the institutions responsible for preparing military leaders. Transforming PME into an innovation-driven space offers a promising pathway to achieving these critical objectives.

In conclusion, addressing the digital deficit in PME requires a multifaceted approach that rethinks traditional instruction, embraces experiential learning, and overcomes institutional resistance. By committing to these changes, PME can become a catalyst for broader organisational transformation, ensuring that armed forces remain agile, adaptive, and capable of meeting the demands of modern warfare. A comprehensive reimagining of PME is essential to securing the military's strategic future and maintaining operational superiority in the digital age.

Acknowledgement:

This work was supported by the Centre of Excellence in Defence, Risk and Resilience (CEDRR) at the University of Portsmouth through the CEDRR R&I Fund for the research 'Future Vision for Professional Military Education'.

References

Alkhazi, B., Alshaikh, M., Alkhezi, S., & Labbaci, H. (2022). Assessment of the Impact of Information Security Awareness Training Methods on Knowledge, Attitude, and Behavior. *IEEE Access*, *10*, 132132–132143. https://doi.org/10.1109/ACCESS.2022.3230286

Altair. (2025, April 14). *Altair Signs MoU with Korea Military Academy to Advance AI Innovation in Defense*. https://altair.com/newsroom/news-releases/altair-signs-mou-with-korea-military-academy-to-advance-ai-innovation-in-defense

Bagiati, A., Kathleen, M., Kennedy, D., Siegel, J., Salazar-Gómez, A. F., Kennedy, K., & Breazeal, C. L. (2024, June). Scenario-based Emerging Technologies Workshop for Military Leaders. *The Future of Engineering Education: 2024 Annual Conference & Exposition*.

Barron, L., & Rowles, P. (2021). *EVALUATION OF DIGITAL LITERACY AS AN AIR FORCE FOUNDATIONAL COMPETENCY*.

Berndtsson, J. (2024). Hybrid threats and the “new” total defence. *Preparing for Hybrid Threats to Security*, 150.

Boladian, R., Daccache, C., Matar, S., & Aggarwal, K. (2024). *Reinventing military education and training for the digital age*. https://www.kearney.com/industry/aerospace-defense/article/reinventing-military-education-and-training-for-the-digital-age

Borghard, E., Montgomery, M., & Valeriano, B. (2021, June 25). *The Challenge of Educating the Military on Cyber Strategy*. https://www.cato.org/commentary/challenge-educating-military-cyber-strategy

Brescia, S. (n.d.). *Navigating the AI battlefield: Opportunities and ethical frontiers*. Retrieved 19 March 2025, from https://www.nrdc-ita.nato.int/newsroom/insights/navigating-the-ai-battlefield-opportunities--challenges--and-ethical-frontiers-in-modern-warfare

Chernikova, O., Heitzmann, N., Stadler, M., Holzberger, D., Seidel, T., & Fischer, F. (2020). Simulation-Based Learning in Higher Education: A Meta-Analysis. *Review of Educational Research*, *90*(4), 499–541. https://doi.org/10.3102/0034654320933544

Chow, A. F., Woodford, K. C., & Maes, J. (2011). Deal or no deal: Using games to improve student learning, retention and decision-making. *International Journal of Mathematical Education in Science and Technology*, *42*(2), 259–264. https://doi.org/10.1080/0020739X.2010.519796

Chromyszak, C., Jacobson, S., Khosraw, E., Lavey, S., Lewis, M., Mabe, S., Olsen, A., Ryals, C., Sahagun, K., & Williamson, I. (2022). *Navigating New Threats: NATO’s Posture on Emerging Technologies*.

Cole, L. (2017). BiblioTech: Closing the Gap between Traditional and Digital Literacy. *Public Library Quarterly*, *36*(3), 244–258. http://10.0.4.56/01616846.2017.1339547

Crilly, M. (2023, July 28). *A post-digital British military – the new influencing arm of the state*. Wavell Room. https://wavellroom.com/2023/07/28/a-post-digital-british-military-the-new-influencing-arm-of-the-state/

Dascalu, D., Ogden, T., Retter, L., & Utting, K. (2024). *Generation Z and Joint Professional Military Education*.

Datta, P. M., & Acton, T. (2023). Did a USB drive disrupt a nuclear program? A Defense in Depth (DiD) teaching case. *Journal of Information Technology Teaching Cases*. https://doi.org/10.1177/20438869231200284

Davis, M. N., & Force, U. S. A. (2021). *Operations in the Information Environment: Achieving Decision Dominance*. School of Advanced Military Studies, US Army Command and General Staff College.

del Castillo Sancho, M. (2023, July 3). *Bridging Boundaries, Building Technology: The Critical Role of Civil-Military Cooperation*. https://www.atlantic-forum.com/atlantica/bridging-boundaries-building-technology-the-critical-role-of-civil-military-cooperation

Devanny, J., Stevens, T., Dwyer, A., & Ertan, A. (2021). *The national cyber force that britain needs?*

Dobson, T., & Willinsky, J. (2009). Digital literacy. *The Cambridge Handbook of Literacy*, *10*, 286–312.

Erbschloe, M. (2017). *Social media warfare: equal weapons for all*. Auerbach Publications.

Farina, A. G. (2022). The Impending data literacy crisis among military leaders. *The Cyber Defense Review*, *7*(4), 91–98.

Fisher, K. M. (2022). Wartime, professional military education, and politics. *International Relations*, *36*(4), 658–681.

Ford, K., & Vignare, K. (2015). The evolving military learner population: A review of the literature. *Online Learning*, *19*(1), 7–30.

Geluk, P., Schlueter, M., Thomas, T., & Erkens, S. (2020). Fixing the talent gap in armed forces worldwide. *Boston Consulting Groups Insights*.

Gilli, A., Gilli, M., & Grgić, G. (2025). NATO, multi-domain operations and the future of the Atlantic Alliance. *Comparative Strategy*, 1–19.
Gilster, P. (1997). *Digital Literacy*. Wiley. https://books.google.co.uk/books?id=awkoAQAAMAAJ
Hasselbladh, H., & Ydén, K. (2020). Why military organizations are cautious about learning? *Armed Forces & Society*, *46*(3), 475–494.
Ivan, C., Chiru, I., & Arcos, R. (2021). A whole of society intelligence approach: critical reassessment of the tools and means used to counter information warfare in the digital age. *Intelligence and National Security*, *36*(4), 495–511.
Jacobs, A. (2016). *Teaching IR at Sandhurst: Blended Learning through an Integrated Approach*. https://www.militarystrategymagazine.com/article/teaching-ir-at-sandhurst-blended-learning-through-an-integrated-approach/
King's College London. (n.d.). *Professional Military Education*.
Lankshear, C., & Knobel, M. (2011). *New literacies: Everyday practices and social learning*. McGraw-Hill Education (UK).
Lewis, J., Powell, A., Roberts, N., & Ward, M. (2024). *Digital skills and careers*. https://researchbriefings.files.parliament.uk/documents/CDP-2024-0073/CDP-2024-0073.pdf
Libel, T. (2021). Professional Military Education as an Institution: A Short (Historical) Institutionalist Survey. *Scandinavian Journal of Military Studies*, *4*(1), 121–131.
Maguire, S. (2021, October 13). Professional Military Education Needs Reform. Here's Why and What to do. *Wavell Room*. https://wavellroom.com/2021/10/13/professional-military-education-reform/
Martin, A. (2008). Digital literacy and the "digital society". *Digital Literacies: Concepts, Policies and Practices*, *30*(151), 1029–1055.
Martin, A., & and Grudziecki, J. (2006). DigEuLit: Concepts and Tools for Digital Literacy Development. *Innovation in Teaching and Learning in Information and Computer Sciences*, *5*(4), 249–267. https://doi.org/10.11120/ital.2006.05040249
MDA Training. (2023, September 26). *Case Studies: Success Stories of Companies Using Simulations for Corporate Training*. https://medium.com/@mdatraining94/case-studies-success-stories-of-companies-using-simulations-for-corporate-training-4216e0f5bc4b
Ministry of Defence. (2022). *Cyber Primer, 3rd Edition*.
Ministry of Defence. (2025). *Fast-track armed forces recruitment launched to boost UK cyber defence - GOV.UK*. https://www.gov.uk/government/news/fast-track-armed-forces-recruitment-launched-to-boost-uk-cyber-defence
Misra, M. (2008). Towards Continuous Military Education in the IAF: A Need for Yesterday. *Air Power Journal*, *3*(1), 77–105.
Morgan McKinley Insights. (2025). *2025 UK Salary Guide* . https://www.morganmckinley.com/uk/salary-guide
Morse, A. (2018). *Ensuring sufficient skilled military personnel*. London: National Audit Office.
Mullen, J., Milechin, L., & Reuther, A. (2019). Proceedings of 2019 IEEE Learning With MOOCS (LWMOOCS) : date and venue, 23-25 October, 2019, Milwaukee, WI, USA. *2019 IEEE Learning With MOOCS (LWMOOCS)*, 150–155.
Onduto, B., Ali, R., & Smed, A. J. (2021). Gamification of Cyber Security Awareness–A Systematic Review of Games. *Computing, Faculty of Technology*.
Prime Minister's Office. (2025, March 12). *Prime Minister: I will reshape the state to deliver security for working people*. https://www.gov.uk/government/news/prime-minister-i-will-reshape-the-state-to-deliver-security-for-working-people
Reforming the civilian workforce - NAO report. (2019, March 8). https://www.nao.org.uk/reports/reforming-the-civilian-workforce/
Sangwan, D., & Raj, P. (2021). The philosophy of Be, Know, and Do in forming the 21st-century military war-front competencies: a systematic review. *Defence Studies*, *21*(3), 375–424.

Sawyer, G., & Emmett, B. (2021). A Review of the Cybersecurity Programs in the United States Army. *Journal of Information and Technology*, *5*(1), 22–30.

Singer, P. W., & Johnson, E. (2022). The Need to Inoculate Military Servicemembers against Information Threats: The Case for Digital Literacy Training for the Force. In *The Great Power Competition Volume 3: Cyberspace: The Fifth Domain* (pp. 283–291). Springer.

Soeters, J. L., Winslow, D. J., & Weibull, A. (2007). Military culture. In *Handbook of the Sociology of the Military* (pp. 237–254). Springer.

Sõmer, T., Ottis, R., & Lorenz, B. (2019). Developing military cyber workforce in a conscript armed forces: Recruitment, challenges and options. *14th International Conference on Cyber Warfare and Security*, 413–421.

Steingartner, W., Galinec, D., & Kozina, A. (2021). Threat defense: Cyber deception approach and education for resilience in hybrid threats model. *Symmetry*, *13*(4), 597.

Sugden, F. (2023, February 17). *Ministry of Defence publishes Science and Technology Collaboration and Engagement Strategy*. https://www.techuk.org/resource/ministry-of-defence-publishes-science-and-technology-collaboration-and-engagement-strategy.html

Thiele, R. (2021). Technology as Driver. *Hybrid Warfare: Future and Technologies*, 59–70.

UK Ministry of Defence. (2021). *Integrated Operating Concept*.

University of Lincoln. (n.d.). *Maritime Studies Centre, BRNC Dartmouth*. Retrieved 19 March 2025, from https://www.lincoln.ac.uk/servicesforbusiness/whoweworkwith/defenceandsecurity/projectselborne/maritimestudiescentre/

University of Portsmouth. (n.d.). *Portsmouth military education*.

Walrond, N. (2024). *Addressing the Digital Skills Shortages in the UK Defence Sector: A Call to Action*. https://www.sandersonplc.com/addressing-the-digital-skills-shortages-in-the-uk-defence-sector-a-call-to-action/

Yamin, M. M., Katt, B., & Nowostawski, M. (2021). Serious games as a tool to model attack and defense scenarios for cyber-security exercises. *Computers and Security*, *110*. https://doi.org/10.1016/j.cose.2021.102450

Zdzikot, T. (2021). Capacity building–how to encourage cyber-experts to join the military? *Cybersecurity and Law*, *4*(2), 37–56.

Chapter 18: Critical thinking – what is it good for?

Lt-Col. Kyrre Tromm **Lindvig**

Abstract:
Critical thinking is a term hailed in many settings. It is being extensively mentioned in management literature (Boyges 2019; Marr 2022), educational literature as well as in within the fields of philosophy and psychology (Lai, 2011). It has also been identified to be a vital skill for military practitioners (Paparone 2014; Toronto 2018). However, several studies do point to the fact that today's military professional military education still has some way to go in including this concept into their teaching. This paper will attempt to show how we can employ a working definition of critical thinking in a military context and why this will be of paramount importance for military personnel, especially in today's fragmented and contested information domain. Special emphasis will be laid upon the use of popular culture as one of several fields of study that can be employed in the training of military personnel in the developing of their critical thinking skills, hardening them against disinformation and fake news.

Key words: Critical thinking, popular culture, information domain, cognitive domain

Introduction

Although the definitions of what critical thinking really is do vary, there seems to be a common thread in that critical thinking is desirable – for business managers, students and among people in general – especially people living in a democracy, as it helps in making informed decisions (Guilliot, 2004). It has also been defined as a vital skill for military practitioners (Paparone, 2014; Toronto, 2018). But how does one define critical thinking? A literature study traces critical thinking to three different strands of thought: The philosophical, the psychological and the educational (Lai, 2011, p. 4). Although the term "critical thinking" has different facets within these different disciplines, Lai finds that there are some main characteristics which catch the essence of what the term signifies: "analyzing arguments, claims, or evidence […] making inferences using inductive or deductive reasoning […] judging or evaluating and making decisions or solving problems […]." (Lai, 2011, p. 9). Although all these traits would seem desirable to see in a person – oneself or another- especially the latter point should be of special interest to the military practitioner – is not solving problems and especially taking decisions what the military is – or at least-should be- all about? Through a literature review, this chapter will argue that the ability to think critically is not sufficiently fostered within professional military education [PME]. Furthermore, this chapter will define the benefits of emphasizing the development of critical thinking for military officers arguing it will increase the ability to cope with today's contested

information domain. Finally, some suggestions and examples of how to introduce more critical thinking into professional military education, using both theoretical works as well as examples from popular culture – a somewhat neglected field of study in military context – will be made.

Do we really teach how to think critically?

Studies suggest that in professional military education, the introduction of critical thinking has not been sufficiently addressed, although the term here often is hailed as a vital skill (Guillot, 2004). In addition, even if there are several military educational institutions that include critical thinking as a part of their curriculum (Parenteau, 2021), studies suggest that this skill is not always transferred to actual military practice. (Antrobus & West, 2022; Sjøgren, 2025). An overview of available literature concerning actual teaching focus within military education seems to suggest a focus on establishing *one* specific way of thinking. As one student put it: "We've been taught what to think but not how to think" (Emilio, 2000, p. iv). This view is being echoed by Antrobus & West (2022), who highlight the inherent dichotomy between where "critical thinking is lauded as a tool to navigate the unpredictability of contemporary warfare" and the reality one encounters in professional military education (Antrobus & West, 2022, p. 78). One of Antrobus and West's examples stem from the higher officer training in the United Kingdom, where they identified the following:

> 'Auto-ethnographic reflection on our experiences of ACSC and Intermediate Command and Staff Course 45 indicates, for example, that their emphasis on the joint operational planning process relies on ensuring students follow generic ways of applying doctrine, rather than questioning that doctrine or the process of its application. Here, the purposely rigid and prescriptive nature of the course collides with the supposedly discursive.' (Antrobus & West, 2022, p. 83).

This is noteworthy as lack of critical thinking seems to have direct ramifications on the efficiency of conducting military operations. In a study analyzing the internal processes of a NATO Headquarters, Søren Sjøgren echoes Antrobus and West, when he found that officers are more prone to adhering to protocol and struggling with managing ever-complex procedures than actually solving the military problems. And this he relates directly to a deficit in the educational background of the officers, since "[…] contemporary PME focuses strongly on the appropriate use of the military planning process and operating the machine, which leads to conservative, standardised solutions." (Sjøgren, 2025, p. 10). Parenteau (2021) traces the issue back to the very nature of military organisations and their intrinsic conservatism, which again is based on their need for consolidation.

Hence, “[m]ilitary organizations generally exhibit a high level of social conformity among members” (Parenteau, 2021, p. 49).

Do we really need critical thinking?

But let us take a step back - how relevant is critical thinking really for military professionals? Can critical thinking even be counterproductive? Here it is important to understand that there is a time and space for everything – there might not be time to engage in long discussions when one is under fire in a trench. However, even in time-critical circumstances, critical thinking might save your life as well – even in the above example you would want to be able to be able to quickly establish where the incoming fire is coming from and not uncritically running straight into the enemy’s machine gun fire. The issue is to have developed critical thinking as a skill that can be used quickly and in a suitable context. And of course, some situations may be better suited than others for employing this skill. In this regard, Parenteau establishes a paradigmatic framework for within which critical thinking will need to adhere to in order to be effective in a military context. These are to: “never undermine the legitimacy of the chain of command […]” and acknowledge “that decision-making is not an exact science’ and lastly, that ‘critical thinking should never undermine the duty to obey.” (Parenteau, 2021, pp. 51-52)

Thomas Williams on his side highlights the effect critical thinking will have on the solving of complex problems: ‘Effective argument ends with a synthesis of all views and stronger collective understanding of the problems’ dimensions before moving on toward identifying solutions.’ (Williams, 2013, p. 52). He furthermore states that: “Critical thinking means the ability to construct and defend an argument using reason, applying intellectual standards of epistemic responsibility, and recognizing and countering logical fallacies as we see them in others and ourselves.” (Williams, 2013, p. 50). Considering for example planning – which is one of the core tasks any officer should be able to undertake – the need for having able, educated personnel that can use their critical reasoning to be able to come up with the best solutions should be of vital interest.

In order to fully appreciate how critical thinking can help the military professional, a look at today’s relentless speed of technological and tactical developments might be helpful. The ongoing war in Ukraine, but also the battles in Nagorno-Karabakh in the 2020s as well as the Israeli incursions into Lebanon and Gaza in 2024-25 show radically changed preconceived notions of how one should – and can fight. The ubiquitousness of drones, developments in space-based command and control, the speed of measure and countermeasure, to name a few -all put the Western military education society at the risk of being overtaken by events and in the worst case,

teaching tactics, techniques and procedures that might be outdated by the time the cadet's graduate. This could have detrimental effects, as

> "[…] the resistance to innovation, and the resulting institutional immobility are highly problematic for organizations that need to adapt to new realities as threats and operational requirements evolve. History books are filled with examples of military powers that were defeated on the battlefield because of their officer's inability or refusal to question their procedures, their techniques, and more fundamentally, their ways of thinking." (Parenteau, 2021, p. 59)

On a positive note, the point that critical thinking can be a way of being able to deal with a rapidly changing military environment has already been known for some time. In effect, Emilio wrote these words over twenty years ago: "We live in a complex world that is both multi-polar and multi-cultural, a world where change is occurring at an ever-increasing pace and where the availability of information now far outstrips any human capability for comprehension" (Emilio, 2000, p. 4). However, not much seems to have happened since then, as Sjøgren's findings show. A multinational divisional NATO headquarters in 2021 uses its doctrinal underlay and its imposed standards, thereby actually limiting innovation in particular and thinking in general: "The wide range of operational possibilities that might exist outside the war machine in military history cannot come into being on the inside; such possibilities do not fit the calculus." (Sjøgren, 2025: 10). This limitation of thought can be detrimental when faced with the increasingly changing developments in military affairs:

> "In the current operational environment, military institutions must remain agile and innovative. To that end, they must rely on an officer corps, which has developed the ability to think critically, so that they may quickly adapt to new realities and introduce changes when needed by criticizing outdated thinking habits." (Paraneau, 2021, p. 54)

The need for critical thinking to be able to identify emergent technological and tactical trends and act in accordance with them might be obvious, even though the examples above show that this skill is not – at least not yet - nurtured to a sufficient degree in our professional military education. However, this paper will argue that critical thinking gains even further importance when we move the discussion over to the cognitive and information domains.

Critical thinking and resilience against disinformation

Today's fragmented media landscape, with AI-generated bots, rampant social media and the incessant increase of partisan reporting, makes it increasingly difficult to navigate in a

seemingly fluid reality. This also makes our societies and our military practitioners vulnerable to influence operations and hybrid actions from malign actors. One example is the Russian regime's expert use of discourse power which has arguably been a major part of his war against the west for decades (Nik, 2025). As an integrated part of Russia's "active measures" against the West, it is a way of waging war under the threshold of armed conflict, but no less lethal in the long run: "Moscow has developed an aggressive campaign to interfere with democratic elections in individual countries and European Parliament elections, co-opt politicians for elite capture, and spread disinformation." (Jones, 2025, p. 9). The Resistance Operating Concept [ROC], published by Joint Special Operations University, further outlines the theoretical background for this campaign. Citing an article by Russian officers Chekinov and Bogdanov, the authors state that:

> "they [Chekinov and Bogdanov] saw the main battleground as the information space. This type of warfare is dominated by psychological and information warfare to crush the morale of enemy troops and the opposing population, thus breaking their will to resist." (Fiala et al., 2020, p. 113)

And this strategy seems to pay off, as we can see in several countries today, where Russian disinformation is being spread, either knowingly or not, by leading opinion makers. (Hoyle & Šlerka, 2024). And the effects are widespread:

> "The Kremlin's messaging has an extraordinary reach: In the first year of the Ukraine war alone, posts by Kremlin-linked accounts were viewed at least 16 billion times by Westerners. Every one of those views is part of a full-spectrum attack against the West designed not just to undermine support for Ukraine, but to actively damage Western democratic systems." (Garner, 2024)

This paper argues that this threat – although deemed less lethal in the short term compared to drones, long-range precision strikes and AI-supported developments on the battlefield – can have a disastrous impact on our societies and more concretely, on the fighting ability of our armies. Since military personnel are just as subjected to disinformation as anybody, the vital task would be to heighten the resilience against the ongoing onslaught we currently are seeing in the cognitive and information domains. And it is here that critical thinking can serve as an antidote, as it will help to identify facts from lies, uncover hidden narratives and also to share these insights among others. Guillot highlights the transparency of critical thinking as one of its major important features: "Being able to coherently explain, illustrate, or elaborate why certain reasoning is faulty is synonymous with teaching critical thinking." (Guillot, 2004, p. 10)

Critical thinking can be taught

After having identified this point of improvement in professional military education this paper will offer some possible pathways to including the training of critical thinking in professional military education. Guillot, who already has worked on this matter in the US, bases his approach on Richard Paul's 8 elements of reasoning, while Lai (2011) refers to several successful instructional programs for college students. Both highlight that critical thinking can be taught, and this competence can be further improved: "The key is to recognize that regardless of the definition, critical thinking abilities can be individually developed." (Guillot, 2004, p. 3). Lai supports this view, stating that: fortunately, many critical thinking researchers maintain that critical thinking skills and abilities can be taught." (Lai, 2011, p. 30). For our purposes, the important point to consider is that critical thinking is not something you either have or have not, rather, it is something which can – and must - be developed over time.

One starting point for developing critical thinking among military personnel would therefore seem obvious: One must introduce the concept of critical thinking early within the professional education. Although one can argue that it is never too late to develop one's own mental and cognitive capabilities, for officers the military academies would be a good starting point. Although military personnel do develop – or should continue to do so – throughout their whole career, the years spent at the military academy seem to have a formative effect on the shaping of their future thinking (Soeters et al., 2006). The military academies offer a good training ground not only due to the formative effect stated above but also that the training of the ability to be able to think critically is a rather time-consuming endeavor, which needs to be conducted over time. The same should be applied to NCOs in their respective training arenas. Michael Guillot states that not only theory, but also practical work is required to master this – as any other new skill:

> "Future critical thinkers must also practice the new skill, so critical thinking becomes second nature as your default thinking pattern. The more you practice thinking using the elements and standards, the quicker your thinking will improve. Initially this practice will be difficult especially as one challenges the mind to think in new ways, remain flexible, open to change, and confront one's ego" (Guillot, 2004, p. 10).

So far, we have identified that military practitioners would benefit from training in critical thinking, and that this skill is trainable. A good starting point for implementing this skill into officers could be to introduce texts from the already mentioned scholars into the curriculum of academies –and some of them already are. In addition, scholars such as Gerras (2008) have established a critical thinking framework to support military decision making. However, this paper will also

highlight another additional method for teaching critical thinking, namely regarding what many do not analyze at all, namely popular culture.

Popular culture as training grounds

As a field of study, popular culture has increasingly been seen as a major field of information about most factors of our society. (Barthes, 1957; Fiske, 1989). Hence, it constitutes a fertile ground for teaching in general and developing critical thinking in particular. Theorists such as Kellner (1995) and Ramonet (2000) have taken this approach one step further and see popular culture as a social field where discourses of power are being manifested, which again makes analyses of popular cultural artefacts such as films, TV and advertising valuable as a way of understanding how our society works.

However, analysis of popular culture has a rather small imprint on the curriculum of military students. Ender et al. trace this back to the epistemological differences between how military culture is studied and how popular culture generally is studied: “These methods are less anchored in the military institution and scholars using these latter techniques are less emic in the military. This disjuncture likely contributes to the lack of synthesis of studies of popular culture and the military.” (Ender et al., 2020, p. 2). However, as it is often from popular culture that people in general and also military personnel draw inspiration and ideas from, this topic should require careful consideration. It is also noteworthy that Ender et al. identified over 100 books and journal articles dealing with the intersection of military and popular culture, making this an area worthwhile delving further into (Ender et al., 2020, p. 1). This paper will argue that analyzing cultural texts from popular culture while employing qualitative techniques from the humanities, will be a way of nurturing critical thinking PME, for cadets, officers and NCOs alike. Christopher Paparone does this with great effect when he uses an allegorical investigation of American football in order to widen the scope of critical thinking to also include the interpretive paradigm as a vital part of it. (Paparone, 2014). As Paparone’s text shows us: Popular culture spans widely - from film via TV, books, sport, games and even fashion. For sake of simplicity, this paper will focus on how complex narratives in film and movies could be fertile training grounds for training the critical thinking muscle.

But in order to do this properly, and to avoid it being only a “movie night”, a theoretical framework will need to be applied. Fortunately, there are several examples to draw upon. One prominent and useful example would be to apply the approach presented in Edward Said’s (1978) *Orientalism*, which deconstructs discursive strategies employed throughout the colonial age, thereby opening up the field of critical thinking towards the complex notions of identity and how it is not a stable, but a highly contested subject. Furthermore, researchers Shohat and Stam (1994)

took Said's approach further in their groundbreaking work on how to better understand one's own identity, using this understanding as a starting point for unveiling other narratives. Central to Shohat and Stam's argument is how everyday sentiment and feeling is generated within popular culture. As an example, they do highlight how many of the epic Hollywood movies about the Vietnam war basically "treat the war as a domestic tragedy", leaving the Vietnamese out as nothing more than nameless killers. (Shohat & Stam, 1994, p. 24). Blockbuster movies in general do offer good analytical training grounds, one example would be the Top Gun franchise, which has been partly made in conjunction with the US Department of Defense and who many pilots to this day claim have been central for their career path: "The film conquered the box office, as well as the hearts and minds of young Americans. Following its release, applications to become Naval Aviators reportedly jumped by 500 percent" (Zenou 2022). Also see Askerøi & Lindvig, (2026) for an analysis of how *Top Gun* aesthetic contributes to its narrative power.

Movies from outside the Hollywood paradigm can also be fertile training grounds for nurturing the ability of critical thinking, as they also offer other cultural prisms that need to be taken into account during the analysis. Examples here could be *Le Crabe-tambour* (1977) and *Diên Biên Phú* (1992) by Pierre Schoendoerffer which both – in very different ways – offer a French perspective on colonial wars and its costs. Mowing further away from the Western cultural canon, the Iranian movie *Oghaba* (1984), is another example worth watching and analyzing. An example of the Iranian regimes "Cinema of Sacred Defense", *Oghaba* is also interesting from a historiological point of view as these movies were made with the explicit goal to bolden Iranian resolve against Iraq during the Iran-Iraqi war (1980-1988) (Lindvig, 2014). One last example this paper will suggest will be the Russian *The Ninth Company* (2005), which follows a group of Soviet Soldiers in Afghanistan in the 80s. This latter movie, being made from a Russian perspective also offers both some compelling and problematic perspectives which could be used e.g. in a debate among cadets.

There would be countless ways of utilizing the above-mentioned examples in critical thinking classes. One could ask the students to read Said's *Orientalism* while viewing in parallel a number of Hollywood-made Vietnam movies. Based on this, one could create guided discussions on the role of constructions of identity in those movies – what is actually being communicated and how? Another possibility would be to ask students to make a comparative analysis of the French and Hollywood-made Vietnam wars – how does the colonial aspect come through in the respective movies? Lastly, a comparative analysis of *The Ninth Company* versus Hollywood Vietnam movies could be a starting point for identifying similarities and differences on how military experience is being narrated from different cultural and political standpoints. The possibilities are abundant,

especially when considering that popular culture spans a lot broader than just movies and films which this chapter has focused on. Most importantly, sessions could be tailored for specific training audiences, depending on how it relates to other items on the curriculum – there is no need to set a strict formula for how popular culture examples could be employed.

Conclusion

In conclusion, this paper has attempted to show the need for critical thinking to be a skill that should be trained as a part of professional military education as it will have beneficial effects on our personnel's understanding of current military conflict, the ability to properly analyze situations and how to plan and conduct military operations. This paper focused on films as one training ground to foster this ability. However, it must be emphasized that the above-mentioned examples of how to use popular culture to foster critical thinking is just one of many ways this ability can be trained. Nevertheless, the main argument of this paper is that the ubiquitous nature of this very culture makes for a compelling, low cost and easy-to-use material for our military students to cut their teeth on. Using examples from popular culture can be used as a way of breaking up longer theoretical sessions on information operations and the cognitive domain. Students could quickly identity with the topic and would easily be able – e.g. though guided discussions to be able to discern and analyze how messages are being promoted throughout these media. The insight gained from these exercises will be a transferable skill, as it will be able to help them to use critical thinking also while being exposed to any form of disinformation, through media or otherwise (Garner et al., 2022). In addition, the skills can be employed as Guilliot stated above, as contributing to a balanced and transparent way of discussion of a wide array of military topics, either related to the ongoing military technological and tactical developments or to improve the processes in the headquarters, which was the subject of Sjøgren's study quoted earlier in this paper. This chapter suggests the discussed examples can be a contribution to developing further ideas on how to keep developing the way we teach critical thinking both in our military academies in particular and throughout professional military education in general.

References

Antrobus, Sophy & West, Hannah. (2022). 'This Is All Very Academic':Critical Thinking in Professional Military Education, *The RUSI Journal*, 167:3, 78-86, DOI:10.1080/03071847.2022.2112521

Askerøi, Eirik and Lindvig, Kyrre Tromm. (2026). "The Sound of Freedom". In Hagen, A.M. & Enstad, K. *Advancing Military Practice through Military Humanities*. Routledge. https://doi.org/10.4324/9781003738886

Barthes, Roland. (1957), *Mythologies.* Éditions du Seuil

Bouygues, Helen Lee. 2019. 3 Simple Habits to Improve Your Critical Thinking, *Harvard Business Review,* published May 2019. https://hbr.org/2019/05/3-simple-habits-to-improve-your-critical-thinking. Site last consulted 17.03.2025

Emilio, George A. (2000). Promoting Critical Thinking in Professional Military Education. *Research Report*. Air Command and Staff College/Air University

Ender, Morten G., Reed, Brian J. and Absalon, Jacob Paul. 2020. Popular Culture and the Military. In Sookermany, A. (ed.) *Handbook of Military Sciences*, 1-19. Springer Cham. https://doi.org/10.1007/978-3-030-02866-4

Fiala, O., Smith K. & Löfberg, A. (2020). *Resistance Operating Concept*. JSOU Press.

Fiske, John. (1989). *Understanding Popular Culture.* Routledge

Garner C., Pennycook G., Rand D.G. (2022): Does Analytic Thinking Insulate Against Pro-Kremlin Disinformation? Evidence From Ukraine. *Political Psychology*, Volume44, Issue1. https://doi.org/10.1111/pops.12819

Gerras, Stephen J. (2006). Thinking critically about critical thinking. A fundamental guide for strategic leaders. *U.S. Army War College*

Garner, Ian. (2024): The West Is Still Oblivious to Russia's Information War. *Foreign Policy*, published 09.03 2024. https://foreignpolicy.com/2024/03/09/russia-putin-disinformation-propaganda-hybrid-war/ Site last consulted 31.03.2025

Guillot, W. Michael. 2004. Critical Thinking for the Military Professional*. Air and Space Power Chronicles*, published 17.06.2004 https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Chronicles/guillot.pdf Site last consulted 24.03.2025

Hoyle, Aiden & Šlerka, Josef. (2024). Cause for concern: The continuing success and impact of Kremlin disinformation campaigns. *Hybrid CoE Working Paper 29.* The European Centre of Excellence for Countering Hybrid Threats.

Jones, Seth G. (2025). Russia's Shadow War Against the West. *CSIS BRIEFS*. March 2025. https://www.csis.org/analysis/russias-shadow-war-against-west Site last consulted 25.03.2025

Kellner, Douglas. (1995). *Media Culture- Cultural studies, identity and politics between the morden and the postmodern.* Routledge

Lai, Emily. (2011). Critical thinking: A literature review. *Pearson's Res Rep*. 6. 40-41.

Lindvig, Kyrre Tromm. (2014): Iransk film i kulturkrigens tegn. *Z Filmtidsskrift*, issue 126. https://znett.com/2014/02/iransk-film-i-kulturkrigens-tegn/ Site last last consulted 23.06.2025

Marr, Bernhard. (2022). 13 Easy Steps To Improve Your Critical Thinking Skills. *Forbes*, published 05.08.2022. https://www.forbes.com/sites/bernardmarr/2022/08/05/13-easy-steps-to-improve-your-critical-thinking-skills/ Site last consulted 17.03.2025

Nik. (2025). The Invisible Arsenal: Russia's Media Machine and the New Face of Conflict". *Stratagem*. Published online 25.03.2025. https://www.stratagem.no/the-invisible-arsenal-russias-media-machine-and-the-new-face-of-conflict/. Site last consulted 26.03.2025

Paparone, Christopher. (2014). Two Faces of Critical Thinking for the Reflective Military Practitioner. *Military Review*. Vol. 94 (6), 104-110.

Paranteau, Danic. (2021). Teaching Professional Use of Critical Thinking to Officer-Cadets Reflection on the Intellectual Training of Young Officers at Military Academies. *Journal of Military Learning*. April 2021. https://www.armyupress.army.mil/Journals/Journal-of-Military-Learning/Journal-of-Military-Learning-Archives/April-2021/Parenteau-Critical-Thinking/ Site last consulted 02.07.2025

Ramonet, Ignacio. (2000). *Propagandes silencieuses*. Gallimard

Said, Edward. (1978/2003). *Orientalism*. Routledge

Shohat, E. & Stam, R. (1994). *Unthinking Eurocentrism – Multiculturalism and the Media*. Routledge

Sjøgren, S. (2025). Entering the war machine: on construction of order in a multinational NATO headquarters. Defence Studies, 1–20.https://doi.org/10.1080/14702436.2025.2477045
Soeters, J.L., Winslow, D.J., Weibull, A. (2006). Military Culture. In: Caforio, G. (ed) Handbook of the Sociology of the Military. *Handbooks of Sociology and Social Research*. Springer, New York, NY. https://doi.org/10.1007/0-387-34576-0_14
Toronto, Nathan W. (2018). *How Militaries Learn: Human Capital, Military Education, and Battlefield Effectiveness*. Lexington.
Williams, Col. Thomas M. (2013). Education for Critical Thinking. *Military Review* January-February 2023, 49-54.
Zenou, Theo. (2022). 'Top Gun,' brought to you by the U.S. military. *The Washington Post*. Published 27.05. 2022. https://www.washingtonpost.com/history/2022/05/27/top-gun-maverick-us-military/ Site last consulted 01.07.2025

Chapter 19: Embracing Digital Transformation in Professional Military Education: Maintaining Relevance, Resilience, and Success

William Combes[1], Capt (ret.), ORCID: https://orcid.org/0000-0003-0191-8203

Abstract:

Military education faces a challenge. The concept of digital transformation, the adoption and integration of digital technologies to enhance learning, operations, and capabilities, is evolving as fast as the underlying technologies that support corporate, education, government, and military institutions' professional practice. An innovative and adaptive evolution is needed to ensure the relevance, resilience, and success of any organisation's underlying vision, mission, and goals. This chapter explores how professional military education (PME) institutions should leverage evolving technologies to improve educational outcomes to create innovative officers capable of excelling in the current technological environment characterised by the rapid evolution of emerging and disruptive technologies and hypotheses that they must embrace this transformation proactively. For the North Atlantic Treaty Organisation (NATO), digital transformation is characterised by the concepts of multi-domain operations, the use of advanced analytics and artificial intelligence to enhance situational awareness, information awareness and decision-making, and fostering innovation and agility by promoting a digital culture and mindset. Educational institutions are pursuing the responsible use of technology and artificial intelligence to tailor and improve educational outcomes, reach broader audiences, and improve faculty capability and efficiency. Military education institutions must do the latter while educating on the former, challenged by the reality that both transformations are mostly conceptual and applicable technological advancements are developing so rapidly. The research will combine a conceptual analysis of NATO military digital transformation and digital transformation at education institutions with a comparative analysis of current, planned, and possible contemporary institutional transformation efforts to identify potential strategies to successfully incorporate emerging technologies into professional development and educational requirements to deliver relevant and timely military education. The study employs a recursive learning methodology that systematically uses AI tools to study AI implementation, while documenting institutional transformation to provide both practical validation and transferable guidance for peer institutions. In other words, recommendations to enable PME institutions to develop faculty and students who are comfortable and skilled with the innovative, ethical, and secure use of technological advancements, including artificial intelligence, in the military domain.

[1] *The author writes here strictly in a personal capacity.*

The research's findings, validated through a comprehensive AI in Professional Military Education workshop with NATO and partner institutions, identify extensive and continuous operational experimentation with new technologies and the wide dissemination of innovative best practices as essential for successful digital transformation. This evidence-based approach ensures the relevance, resilience and success of military education institutions and their alumni.

Key words: Digital Transformation, Professional Military Education (PME), Emerging and Disruptive Technologies (EDTs), Artificial Intelligence (AI), NATO Digital Transformation, Multi-Domain Operations (MDO), Advanced Analytics, Ethical AI, Adaptive Learning, Operational Experimentation, Faculty Development, Critical Thinking, Resilience in Military Education Institutions.

Introduction[2]

The rapid pace of technological advancement in computing speed, digital communication bandwidth, and artificial intelligence is spurring organisations of all types to pursue, alter, or accelerate their business practices to leverage the increased capabilities. Digital Transformation, the adoption and integration of digital technologies to enhance organisational or personal capabilities, learning, and operations, is evolving as fast as the underlying technologies. An innovative and adaptive evolution is needed to ensure the relevance, resilience, and success of any organisation's underlying vision, mission, and goals. This is true for professional practice in industry, academia, government, and military institutions.

For the North Atlantic Treaty Organisation [NATO], *Digital Transformation* is a response to the advancing capabilities and possible proliferation of emerging and disruptive technologies [EDT]. NATO characterises this transformation by employing multi-domain operations, using

[2] There is a parallel story to the research narrative. This involves a working group established by the Baltic Defence College entitled the Digital Transformation and Artificial Intelligence Working Group (DTAIWG), that the author chairs. In our annual quality report to NATO for 2023, we stated the purpose of DTAIWG is:

> '… investigating two paths. The first path is to continue and expand the education of our students on innovative capabilities and concepts developed to counter or exploit emerging and disruptive technologies to understand their impacts on the character of warfare and how to implement them to ensure our defence and security. The second path is to ensure that our faculty has the necessary skills, knowledge, and digital tools to deliver this evolving technology education specifically and to leverage technological solutions to improve the development and delivery of all our education.'

In the spirit of experimentation, the DTAIWG has been actively using AI tools to develop the necessary skills to educate the faculty and students on AI, inform policy, and see its capabilities in helping us perform our duties. In my case, it included the use of what I will call virtual interns to assist in researching and writing DTAIWG products and this chapter. The interns include, to varying degrees, Microsoft Copilot, Perplexity, Google Gemini, Open AI ChatGPT, Grammarly, Writefull, and to a lesser extent, Research Rabbit, Elicit, and others. This assistance will be documented in footnotes throughout the chapter. The abstract was written by me. The draft was submitted to Perplexity for recommendations on improvements. A human reviewer (my wife, a university professor) read my abstract and the AI assistants' advice. Her only comment was that I should follow AI's guidance. The link to the Perplexity conversation: https://www.perplexity.ai/search/what-is-your-opinion-of-this-a-0hjaxrFtRyie7QY.MOrVDQ

advanced analytics and artificial intelligence to enhance situational awareness, improving information awareness and decision-making, and fostering innovation and agility by promoting a digital culture and mindset. NATO and its member nations are developing these concepts.

Academic institutions are pursuing the responsible use of technology to tailor and improve educational outcomes, reach broader audiences, and strengthen faculty capability and efficiency. This digital transformation and innovation in the education sector began long before it was accelerated to facilitate mandatory or necessary remote and hybrid learning in response to COVID-19. Now, with the rapid capability advancement of text-generating artificial intelligence, large language models and AI powered decision-making models, this digital transformation is re-accelerating.

The challenge for professional military education [PME] institutions is that they must do the latter (*transform themselves*) while also developing faculty and educating students on the former (*NATO's Digital Transformation efforts*). This challenge is exacerbated by the reality that both transformations are primarily conceptual, and applicable technological advancements are rapidly developing.

This chapter explores how PME institutions should take advantage of evolving technologies to improve educational outcomes and create innovative officers capable of excelling in the current technological environment characterised by the rapid evolution of emerging and disruptive technologies. It also hypotheses that they must embrace this transformation proactively.

The research will combine a conceptual analysis of the digital transformation of NATO military operations and the digital transformation of education institutions with a comparative study of current, planned and possible institutional transformation efforts to identify potential strategies to successfully incorporate emerging technologies into professional development and educational requirements to deliver relevant and timely military education. In other words, recommendations to enable military educational institutions to develop faculty and students who are comfortable and skilled in the innovative, ethical, and secure use of technological advances, particularly artificial intelligence, to enhance their performance in the academic and military domains.

The research's findings expect to identify extensive and continuous operational experimentation with new technologies,[3] and the wide dissemination and sharing of innovative best practices and lessons learned,[4] will be necessary to ensure a successful digital transformation and the relevance, resilience and success of military education institutions and their alumni. How the

[3] See footnote 2.
[4] For example, presenting this research at the International Society of Military Sciences 2024 Conference at the Swedish Defence University, Stockholm, Sweden.

Baltic Defence College, a PME institution of the three Baltic states (*Estonia, Latvia, and Lithuania*), is implementing these recommendations will also be shared before the conclusion.

NATO Digital Transformation.

The concept of digital transformation has evolved since the middle of the twentieth century (Vial, 2019). The invention and subsequent improvements to semiconductors allowed information digitisation, a concept that Shannon and Weaver envisioned in *A Mathematical Theory of Communication* (Shannon & Weaver, 1959). More powerful computers are now ubiquitous, with many of us carrying mobile phones with the computing power of mainframe computers from the turn of the century.[5] Digital transformation is innovation using digital technology – how to create new products or processes to solve, improve or capitalize on the problem or opportunity at hand.[6]

For industry, this means using digital technology to deliver customer value through improving efficiency and reducing costs using automation, enhancing customer relations via advanced analytics and communication, and responding to customer needs and market changes through innovative and evolving business models, practices, and products. (Vial, 2019). Regarding educational institutions, including PME, digital transformation aims to improve the quality, accessibility, and relevance of education; its fundamental purpose is adapted to an increasingly digital world of cloud computing, the Internet of Things, mobile technologies, big data analytics, machine learning, and artificial intelligence. This digital transformation in education will be explored further in the next section.[7]

For the North Atlantic Treaty Organisation [NATO], *Digital Transformation* is a response to the advance in capabilities and the possible proliferation of emerging and disruptive technologies [EDT] (NATO ACT, 2023; NATO STO, 2023). Some EDTs, such as artificial intelligence, are also part of the solution. NATO's vision for this transformation includes the use of multi-domain operations, the use of advanced analytics and artificial intelligence to improve situational awareness, improve information awareness and decision-making, and foster innovation and agility by promoting a digital culture and mindset. NATO and its member nations are developing these

[5] A reverse citation, my own statement fed into Perplexity to find sources: https://www.perplexity.ai/search/how-does-the-computing-power-o-gaNUrCqcTZmZ8j10TwOrmQ.
[6] Perplexity does not like my definition of Digital Transformation and thinks it should be expanded to 'Digital transformation is the process of integrating digital technologies into all areas of a business to fundamentally change how it operates, innovates and delivers value to customers. It encompasses transforming products, processes, culture and customer experiences to meet evolving market demands. The goal is to increase competitiveness through innovation, improved efficiency and enhanced customer value in an increasingly digital world.' https://www.perplexity.ai/search/is-this-a-good-definition-of-d-Q2ILjjrBTfS_QJM7OCoghA.
Either is better than the synthesized definition in Vial, 2019: 'a process that aims to improve an entity by triggering significant changes to its properties through combinations of information, computing, communication, and connectivity technologies'
[7] A discussion with perplexity regarding digital transformation in the academic and business contexts: https://www.perplexity.ai/search/academic-definitions-of-digita-KuSRmpAPRjGpumj2te2dSg.

concepts as described in NATO's 2022 *Strategic Concept* and NATO's *Warfighting Capstone Concept* (NATO, 2022; NATO ACT, 2021). [8]

The NATO approach to emerging and disruptive technologies [EDTs] is to develop and adopt new technologies to improve its defence and deterrence capabilities while ensuring their responsible and ethical use. NATO endorsed a strategy on EDTs which outlines some particular objectives (NATO, 2024). NATO must promote and protect the development of technologies and its relevant technological edge for its core tasks and missions. This development must be based on solid principles and standards for responsible use of these technologies, while considering the values of NATO and international law. It is necessary to improve NATO's innovation system and innovative culture and to reinforce the transatlantic industrial and technological base. We must raise awareness and understanding of opportunities, challenges, and threats to anticipate and respond to technological advancements. Lastly, this will require engaging with partners, academia, the private sector, and civil society on EDTs and promoting cooperation and dialogue with other international organisations.

Some EDTs that NATO focuses on include data, artificial intelligence, autonomy, quantum technologies, biotechnology and human enhancement, hypersonic technologies and space. NATO recognises that these technologies can provide new opportunities for NATO militaries, such as improving situational awareness, decision-making, resilience, efficiency, and sustainability. However, these technologies also represent new threats from state and nonstate actors, both militarily and to civilian society.

The NATO EDT approach is part of the NATO 2030 agenda, which aims to make the alliance stronger, more resilient, and more adaptable to the changing security environment. The NATO EDT approach is driven by improved collaboration with leading voices in the public, private and academic sectors on technologies and their implications. NATO is also engaging with other international organisations, such as the European Union and the United Nations, to address the global challenges and opportunities posed by EDTs (NATO, 2021).

To implement its EDT strategy, NATO has launched several innovation initiatives, such as the Defence Innovation Accelerator for the North Atlantic [DIANA], a network of test centres and accelerator sites that will support the development and adoption of innovative technologies across the Alliance. NATO has also established a multinational venture capital fund, the NATO Innovation Fund, which will invest in start-ups and small and medium-sized enterprises to develop cutting-

[8] In the NATO section, summaries of cited NATO documents and websites were analyzed using Microsoft Copilot in a Microsoft OneNote notebook. Copilot was used to make bullets for PowerPoint slides (also using Copilot inside of PowerPoint) and assist in preparing presentation notes for DTAIWG briefs and educational material for visitors, faculty, and students. All this was used for drafting this section.

edge technologies for defence and security. In addition, NATO has created an EDT advisory group, which consists of 12 experts from academia and industry who provide external advice and recommendations to NATO on its EDT efforts (NATO, 2024). The findings and capabilities of these initiatives need to be shared to educate and equip the Alliance.

Regarding AI, the NATO Artificial Intelligence Strategy is a document that outlines the Alliance's vision, objectives, and principles for developing and using AI responsibly for defence and security purposes. The Allied defence ministers formally adopted the Strategy in October 2021 with four main aims. The first is to provide a foundation for NATO and allies to lead by example and encourage the development and use of AI responsibly for Allied defence and security purposes. Another aim is to accelerate and mainstream AI adoption in capability development and delivery, enhancing interoperability within the Alliance through proposals for AI Use Cases, new structures, and new programmes. We must also protect and monitor our AI technologies and ability to innovate, addressing security policy considerations such as operationalising the Principles of Responsible AI Use. The last aim is to identify and protect against the threats from malicious use of AI by state and non-state actors (NATO, 2021).

As mentioned in the objectives, the strategy also defines six principles of responsible use of AI in defence, which must be factored into AI education. The use of artificial intelligence must be lawful, responsible and accountable, explainable and traceable, reliable, governable, and must mitigate bias. The use of AI must comply with international law and NATO policies and standards. Human responsibility and accountability must be ensured through appropriate human oversight and control mechanisms. Its use must be explainable and traceable, ensuring the transparency and verifiability of AI systems and their outcomes. Defence AI must be reliable, ensuring the quality, safety, and robustness of AI systems and their outcomes. The use of AI must be able to provide the ability of human intervention to correct AI systems and their outcomes when necessary. The use of AI in defence must mitigate bias, ensuring fairness, inclusiveness, non-discrimination, and outcomes (NATO, 2021).

The strategy also highlights the importance of cooperation and collaboration among Allies, as well as with the private sector and academia, to leverage the potential of AI while safeguarding against its malicious use by state and nonstate actors. It also recognises the leading role of the civil private sector and academia in AI development and calls for regular high-level dialogues, engaging technology companies at a strategic political level to be informed and help shape the development of AI-fielded technologies, creating a common understanding of the opportunities and risks arising from AI.

As a PME institution working for NATO countries, the implications of NATO's concept of digital transformation would then add an element of education on the specific transformation and innovation paths proposed and approved by the political leaders of these countries. These include multi-domain operations, using big data and AI responsibly to support decision-making, fostering innovation and agility, and promoting a digital culture and mindset. This implies experimentation since some of the concepts are not fully developed, such as multi-domain operations and how to use artificial intelligence in decision-making, leadership, and management. It also implies collecting best practices and lessons learned from others experimenting with technology. Sources for these emergent practices include the NATO innovation bodies mentioned above, other governmental, academic and industrial institutions involved in defence capability research and development, the real-world experiences of our allies and partners, and analysis of the use of technology by potential adversaries.[9]

Digital Transformation in Education

Educational institutions are seeking the responsible use of technology to tailor and improve educational outcomes, reach broader audiences, and improve faculty capability and efficiency through innovation. This digital transformation in the education sector, or educational innovation, began long before it was accelerated to facilitate mandatory or necessary remote and hybrid learning in response to COVID-19. Now, with the rapid capability advancement of text-generative artificial intelligence large language models, this digital transformation is accelerating once again (Martin & Xie, 2022).

The United Nations Educational, Scientific and Cultural Organisation [UNESCO] guidance on generative AI [GenAI] in education and research provides a comprehensive framework aimed at promoting ethical and effective integration of AI technologies. Released on 7 September 2023, the document emphasises the need for a human-centred approach that prioritises inclusivity, equity, and the enhancement of human capabilities.

The UNESCO guidance on the ethical use of GenAI in education outlines a comprehensive framework that emphasises interactive participation, higher-order thinking skills, human accountability, inclusive access, collaboration, and rigorous evaluation. It addresses ethical concerns such as data privacy, bias, and regulatory gaps, recommending practical steps for implementation, including stakeholder engagement, domain-specific application, pedagogical

[9] For example, CNAS The Role of AI in Russia's Confrontation with the West, while there may be a gap between its ambitions and current capabilities, Russia considers AI in warfare to be pivotal and is investing appropriately. https://www.perplexity.ai/search/summarize-pchz_8wsRO6Y6zELMTMM_w; and RUSI Occasional Paper by Balis and O'Neill, 2022, Trust in AI: Rethinking Future Command.

guidance, and thorough impact assessment to ensure AI enhances learning while promoting equity and inclusivity (Miao, 2023).[10]

Educational institutions are increasingly leveraging AI in various ways to improve education and research.[11] Personalised learning is one significant area where AI makes a difference. Adaptive learning platforms tailor lessons, assignments, and learning paths to the needs of each student by analysing performance data to identify strengths, weaknesses, and learning styles. Intelligent Tutoring Systems [ITS] act as virtual tutors, providing step-by-step guidance and individualised feedback, adapting to the student's pace, and offering hints or explanations as needed.

AI also assists teachers by automating grading for tasks with definitive answers and even providing feedback on open-ended questions and essays, thus reducing their workload. Administrative tasks such as attendance tracking, report generation, and classroom scheduling are streamlined by AI, allowing educators to focus more on student interaction. Additionally, AI can analyze student data to identify patterns and those at risk of falling behind, enabling teachers to offer proactive support.

In content creation and curation, AI tools help generate lesson plans, practice questions, and other educational materials. Personalised content recommendations guide students to relevant resources based on their learning profiles and interests, helping them discover more pertinent materials. AI improves accessibility and inclusivity through assistive technologies such as text-to-speech for visually impaired students, speech-to-text for those with limited mobility, and real-time translation for language learners. Interactive AI-powered games teach basic academic skills and concepts to young learners in an engaging way.

In research, AI excels at analysing large datasets, identifying patterns, correlations, and potential insights that humans might take much longer to uncover. Predictive modelling by AI helps predict student success, areas for curriculum improvement, and potential interventions to maximise learning potential. AI-powered tools help with systematic literature reviews, sorting through large amounts of academic papers to identify trends and research gaps.

Recent research demonstrates that artificial intelligence is transforming higher education in multiple, interconnected ways. Foundational work, such as the 2020 IEEE review, documents how AI-powered adaptive learning systems personalize instruction, automate assessment, and support student engagement at scale, laying the groundwork for more responsive and effective

[10] Rephrasing of Microsoft Copilot summary of the reference.
[11] Microsoft Copilot in Word rephrasing of a google Gemini discussion: https://gemini.google.com/app/b75ba17f78183bcf. Content of the discussion checks with numerous articles available on Harvard Business Review Education website (Harvard Business School Publishing, 2024).

educational practices (Chen, 2020). Building on this, a 2025 systematic review highlights the expanding role of AI in supporting self-regulated learning, providing adaptive feedback, and enabling new forms of student autonomy through chatbots, intelligent tutoring systems, and dynamic learning environments (Lan, 2025).

Universities are actively responding to these trends. The University of Oxford has established dedicated task groups and published comprehensive guidance to support the ethical and effective integration of AI in teaching, learning, and assessment, with a strong focus on faculty development and student support (University of Oxford, 2024; University of Oxford Centre for Teaching and Learning, 2023). The University of Tartu, meanwhile, has implemented national and institutional policies, developed training programs, and conducted research initiatives to foster AI readiness among staff and students, while also engaging in international dialogue on best practices and ethical considerations (University of Tartu, 2023; Lepkin, 2025).

These institutional approaches to AI integration align with emerging practitioner wisdom about effective human-AI collaboration. Ethan Mollick of the Wharton School of Business at the University of Pennsylvania has published blog posts, articles, and a book on how generative AI can improve human academic or otherwise performance. In his book, Co-Intelligence, and his blog posts, he suggests that you should always invite generative AI to assist with your work to assess its strengths and weaknesses. You should treat these tools as humans but tell them what kind of person they are (*prompt engineering*). You should be the actual human in the loop, letting AI handle tasks that it is good at (*and doing the ones you are good at yourself*). Since they are improving so rapidly, the AI you work with today is the worst you will ever use. He refers to the improving nature of what AI is and is not good at as the jagged frontier (Mollick, 2024).[12] Experimentation is key to exploring this frontier.

However, we must systematically address important considerations. Ethical concerns include issues of bias in AI algorithms, data privacy, and ensuring equitable access to AI-powered tools in education. The truthfulness of responses and the voracity of references are also concerns. Collaborating with educators is crucial for the successful integration of AI technologies, ensuring that these tools enhance and support their pedagogical approach rather than replace it. And, of course, learning outcomes must be achieved and academic integrity must be ensured (European Commission, 2022). The next section will examine the progression of PME in relation to both the beneficial and challenging aspects of digital transformation and artificial intelligence.

[12] In addition to his book, Professor Ethan Mollick's blog/newsletters have interesting content regarding the use of AI in education, as well as ongoing analysis of the jagged frontier. One Useful Thing: https://www.oneusefulthing.org/about; and More Useful Things: https://www.moreusefulthings.com/.

Professional Military Education[13]

The Baltic Defence College is an English-language, NATO accredited PME institution of the three Baltic states, Estonia, Latvia, and Lithuania. The college educates officers, senior non-commissioned officers, and government civilian servants of the three nations and those of NATO and NATO partners at the operational and strategic levels. The development of critical thinking, communication, and leadership skills is the objective of our course curriculums. In line with our framework nations and NATO expectations, we also focus on increasing contemporary content supporting NATO Digital Transformation efforts: multi-domain operations, artificial intelligence, digitisation, and innovation. We are also actively incorporating recent lessons identified and lessons learned across our academic portfolio, particularly those from Russia's ongoing invasion and war in Ukraine.

To ensure the incorporation of these important topics into the curriculum in an educationally sound manner, the Baltic Defence College established the Digital Transformation and Artificial Intelligence Working Group [DT/AI Working Group, DTAIWG] with members from across the faculty and staff of the college, under the author's leadership. The working group has two missions. The first is to expand the education of students on innovative capabilities and concepts designed to counter or leverage emerging and disruptive technologies, thereby understanding their impacts on modern warfare and their implementation for defence and security. The second is to ensure that faculty members have the necessary skills, knowledge, and digital tools to deliver this evolving technology education effectively and to incorporate technological solutions to enhance the overall educational experience to develop our students' abilities to apply critical thinking to the use of AI as they use it to improve their critical thinking.[14]

In other words, the DT/AI Working Group was to determine what was in the realm of the possible regarding education tools and AI, develop a strategy to bring those possibilities to fruition, and report progress to the framework nations (*our primary stakeholder*) and NATO (*as part of our certification that our education is constantly improving and adapting to meet NATO needs*) - **process, findings, and products**.

The working group collected data on where innovation and military technology have been incorporated in the past, including a weeklong module for the operational-level Joint Command and General Staff Course' Innovation and Military Technology' that has been included in the

[13] At one of the first meetings of the DTAIWG, Microsoft Copilot within Word was used to develop two white papers to facilitate the team's brainstorming on the topic. These were on Digital Transformation in Military Education and Artificial Intelligence and Military Education: Opportunities and Risks. These reveal the capabilities of AI at the start of the journey as well as potential pitfalls, including challenges related to student education and written assignments.

[14] This paragraph is an edited Microsoft Copilot in Word paraphrasing of the paragraph introducing the DTAIWG in the first footnote to the Introduction.

curriculum since at least 2018. It was clear that future concepts included in this module would need to be brought forward into the curriculum as they developed real-world applications and lessons learned. This includes topics such as autonomous vehicles, artificial intelligence, OSINT tools, etc.

The group also began to experiment with artificial intelligence and other educational tools and encouraged other faculty members to do the same. During this process, it became clear that the command policy on the use of AI would need to be adjusted. Although it gave faculty and students the ability to use AI as part of the education process while considering the ethical implications mentioned earlier in the article, students felt the policy was too restrictive. Therefore, they were afraid to use it unless specifically encouraged by individual faculty members (*mostly members of the DT/AI working group*).

Our assessment revealed that the faculty were not using the full capabilities of the digital tools they already had at their disposal and were also too busy to explore those capabilities or search and experiment with new tools. During this period (*spring semester 2023*), Microsoft added Copilot generative AI to Edge as part of our educational licence. Instantly, a capable AI was available to all faculty and students, and we needed to accelerate AI experimentation for both faculty and students.

The systematic approach required that this experimentation and the collection and dissemination of our lessons learned regarding e-tools and artificial intelligence would need to be augmented by the lessons learned from other education professionals. This is a nearly continuous process as AI continues to mature and the jagged edge of what it is and is not good at continues to change. This is analogous to other future and current technology topics where we are not doing the experimentation, such as Ukraine's lessons learned regarding aerial drones or the latest developments regarding the multi-domain operations concept.

This chapter, along with the Digital Transformation and Artificial Intelligence Working Group, advocates for extensive and continuous operational experimentation with new education, productivity, and communication technologies, including those powered by artificial intelligence, in an ethical and responsible manner. Furthermore, it emphasizes the necessity of widely disseminating and sharing innovative best practices and lessons learned to ensure successful digital transformation. Such efforts are critical for maintaining the relevance, resilience, and success of military education institutions and their alumni.

As a result, the working group proposed and staffed, and the Commandant of the Baltic Defence College approved, a directive on Digital Transformation and Artificial Intelligence (appendix 1). This promulgates a mission to '… develop staff and students who are appropriately skilled in the innovative, ethical and secure use of AI and other technological advances to expand

their critical thinking and improve their performance in the educational and military domains.' Conceptually, the mission will be achieved through the education of staff and students about tools, capabilities, and ethical use (*including security and academic integrity*), faculty and students, experimentation, and the collection and dissemination of best practices. It also acknowledges that the assessment of the achievement of learning outcomes may need to be reevaluated, particularly when it comes to written assessments.

A new Policy on the Use of AI in Education was proposed, staffed, and signed into use. This new policy (appendix 2) encourages experimentation while ensuring ethical use and academic integrity. It provides examples assistance that AI could give, such as:

- When doing independent work, to get explanations of concepts, find ideas, improve text, or ask self-check questions.
- To overcome writer's block or the so-called fear of the blank page.
- As a brainstorming assistant.
- As a programming aid.
- For translating texts.
- For developing critical thinking by evaluating its responses to queries.
- To get a general overview of a large amount of material (summarizing texts, data).
- To evaluate or assess a draft work and ask for recommendations on how to improve it.

It also explains that the use of AI must be transparent and properly acknowledged to ensure academic integrity and the achievement of learning outcomes. It must also ensure that privacy and security regulations are upheld.

Faculty and students were educated on the directive and use policy, prompting strategies, the good and bad qualities of AI as it exists today, and encouraged to experiment and share their lessons learned and best practices. [15] Building on these foundational insights, BALTDEFCOL hosted a comprehensive AI in Professional Military Education workshop in February 2025, bringing together representatives from NATO institutions, partner academies, and defense organizations. The workshop validated the recursive learning methodology while generating concrete best

[15] Prior to developing the comprehensive AI collaboration system described in the next footnote, initial publication formatting assistance was provided by simpler AI tool interactions. The publication template and final draft (of which this was the last substantive paragraph before the conclusion) were loaded into agents in Perplexity and Copilot to recommend required changes for format compliance and technical guidance. You can see the Perplexity discussion here: https://www.perplexity.ai/search/feedback-on-this-paper-recomme-QtIFSLCbQ0GlswDdinnYhQ?login-new=false&login-source=requestAccessLoginGate. Microsoft 365 Copilot provided encouraging peer-review style feedback, noting the paper's clear structure, comprehensive coverage, and alignment with template guidelines, while suggesting minor improvements such as adding tables or figures and ensuring proper AI tool citations. This early-stage AI assistance demonstrated the potential for more sophisticated collaboration approaches later implemented.

practices for AI integration across military education institutions. Workshop outcomes directly informed development of BALTDEFCOL's detailed digital transformation roadmap and institutional policy refinement, demonstrating how systematic experimentation creates transferable frameworks for military organizations implementing human-AI collaborative approaches.

Since the initial development of this framework, similar initiatives have been documented across other peer institutions, suggesting the timeliness of the approach and its broader applicability. The U.S. Army War College uses AI-powered analytics to continuously refine its curricula while carefully enforcing policies on generative AI use (Barry & Wilcox, 2024). The NATO Defence College integrates AI-assisted multi-domain simulations to improve strategic decision-making and prepare leaders for complex security challenges (NATO Defence College, 2024). Meanwhile, the Korea Military Academy (KMA), in partnership with Altair, employs AI-driven simulation software to advance defence innovation, train future leaders, and enhance complex scenario modelling (Altair, 2025). Though approaches differ, all share a commitment to preserving academic integrity while strengthening decision-making capabilities - principles central to the BALTDEFCOL methodology developed here.

The effectiveness of these principles in practice is demonstrated through comprehensive assessment of BALTDEFCOL's experimental approach. Surveys of 36 staff and 51 students provide concrete evidence of systematic progress and validate key theoretical foundations underlying the methodology. Survey data demonstrates that 64.7% of students view AI integration as "essential in modern PME," while 82.35% find institutional policies appropriately balanced, confirming the effectiveness of iterative policy development. Staff who actively engage with AI tools report "very effective" to "extremely effective" outcomes for research, content creation, and administrative efficiency, validating the practical benefits of systematic implementation. These efficiency gains translate directly to enhanced operational tempo and decision-making speed - critical capabilities for contemporary military operations requiring rapid adaptation to evolving threats.

Critical student feedback revealed a key insight: "Most AI avoid military topics," highlighting both the specialized requirements of military education and validating the strategic focus on domain-specific applications central to our approach. This capability gap reinforces the strategic necessity for developing specialized AI applications that can support classified military planning, threat assessment, and operational decision-making in contested environments. This evidence also supports Mollick's observation that effective AI collaboration requires significant learning investment - approximately 10 hours of hands-on experience to develop necessary prompting skills and understand AI's "jagged frontier" of capabilities and limitations. This learning requirement has

direct implications for military professional development programs, as commanders must understand AI capabilities and limitations to effectively employ AI-enabled systems in operational contexts.

Constructive institutional feedback, including observations that "digital transformation are loud words" without addressing fundamental processes, validates the iterative improvement methodology rather than undermining it, directly informing policy refinement and demonstrating the framework's responsiveness to operational realities. These measurable outcomes provide empirical foundation for a transferable methodology while highlighting areas requiring continued development and institutional capacity building.

Methodology: Recursive Learning Through Human-AI Collaboration

The approach developed throughout this analysis and documented in the footnotes represents what can be termed "recursive learning methodology" - systematically using AI tools to study AI implementation while documenting institutional transformation. This methodology evolved through three distinct phases, culminating in an AI partnership that embodies the institutional digital transformation vision itself.

Initial methodology development began with personal exploration of AI tools for research and writing support, deploying "virtual interns" (Microsoft Copilot, Perplexity, Google Gemini, OpenAI ChatGPT, Grammarly, Consensus, Writefull, et al) to assist in researching and writing DTAIWG products and early draft portions of this manuscript. The approach emphasized maintaining human oversight while exploring AI capabilities for literature synthesis, draft improvement, and fact-checking, establishing foundational principles for responsible academic use, etc. This individual experimentation phase directly supports NATO's emphasis on fostering innovation and digital culture, establishing the human capital foundation essential for multi-domain operations.

The methodology then expanded to institutional-wide implementation. Students were encouraged to use AI tools transparently for concept explanation, idea generation, text refinement, brainstorming assistance, and developing critical thinking through evaluation of AI responses. Faculty explored applications in course preparation, research support, and administrative efficiency. The institutional implementation validates NATO's principle that AI integration must enhance rather than replace human decision-making capabilities, particularly for command authority in complex operational environments, and for education.

The methodology culminated in developing an AI partnership that represented the digital embodiment of the Baltic Defence College's comprehensive transformation roadmap. Rather than

using generic AI tools, this approach created a digital manifestation of institutional strategic frameworks, communication patterns, project management methodologies, and systematic implementation approaches developed through the Digital Transformation and AI Working Group. This coordinated AI ecosystem approach validates that successful institutional digital transformation requires developing AI partnerships as integrated systems reflecting organizational identity and strategic vision rather than isolated technological capabilities. The multi-platform methodology demonstrates that sophisticated AI orchestration, maintaining human command authority while leveraging diverse AI capabilities, represents the practical realization of human-centric technology integration principles. The embodied partnership phase demonstrates practical realization of NATO's vision for human-AI collaboration in defense contexts, where AI augments strategic thinking while maintaining clear human command responsibility.

The methodology progression from individual experimentation through institutional implementation to embodied partnership provides a replicable framework for other military education institutions and for student education on the use of these tools. Key principles include transparent AI acknowledgment, systematic progression from personal experimentation to institutional adoption, continuous assessment and iteration, and developing AI partnerships that reflect individual or organizational identity and strategic vision. This progression directly supports NATO transformation objectives by ensuring military leaders understand both AI capabilities and their role in maintaining human command authority in AI-enabled operational environments.

Conclusions

PME institutions, like many corporations and civilian organisations, large or small, must systematically engineer solutions to leverage technology and artificial intelligence to their benefit. This article explored how PME institutions such as the Baltic Defence College should take advantage of evolving technologies to improve educational outcomes and create innovative officers capable of excelling in the current technological environment characterised by the rapid evolution of emerging and disruptive technologies. It hypothesised that they must embrace this transformation proactively.

The chapter analysed NATO military digital transformation, explored how educational institutions are transforming to the rapid advance of digital tools, including artificial intelligence, and looked at the Baltic Defence College's efforts at digital transformation to identify potential

strategies to successfully incorporate emerging technologies into professional development and educational requirements to deliver relevant and timely military education. Since this framework's initial development in August 2024, the emergence of similar initiatives across NATO institutions validates both the strategic foresight of early adoption and the transferable nature of the methodology. The U.S. Army War College's AI-powered analytics, NATO Defense College's AI-assisted simulations, and Korea Military Academy's AI-driven modelling represent convergent evolution toward principles central to the approach developed here: preserving human judgment while enhancing decision-making capabilities through systematic AI integration.

This research contributes a systematic three-phase methodology progressing from individual experimentation through institutional implementation to embodied AI partnership. The recursive learning approach - using AI tools to study AI implementation while documenting transformation - provides both practical validation and transferable guidance. The methodology's evolution from basic tool use to sophisticated collaborative partnership demonstrates the potential for developing AI systems that embody institutional strategic vision rather than merely providing generic technological support. The coordinated use of multiple AI platforms reflecting organizational identity and strategic vision validates that successful institutional digital transformation requires developing AI partnerships as integrated systems rather than isolated technological capabilities.

The research provides actionable recommendations for other PME institutions to continue wide-ranging operational experimentation with AI solutions and systematic dissemination of innovative best practices. This evidence-based approach validates that PME institutions must develop AI integration frameworks that enhance rather than replace human critical thinking, maintain clear command authority structures, and align technological capabilities with institutional mission requirements in order to develop faculty and students who are comfortable and skilled in the innovative, ethical and secure use of technological advancements, including artificial intelligence, to improve their performance and decision-making in the academic and military domains.

The methodology presented here offers a framework for achieving digital transformation objectives while positioning institutions as regional leaders in responsible AI adoption. The paper suggests that both are necessary to ensure that the Baltic Defence College and other PME institutions continue to provide relevant education, develop resilience in the face of technological progress, and contribute to the success of the institution and, most notably, its alums as they lead their nations to navigate a technology-driven volatile, uncertain, complex, and ambiguous future security environment.

BALTIC DEFENCE COLLEGE
THE COMMANDANT

DIRECTIVE

Directive number: 3 / 14.08.2024
To: BALTDEFCOL
Subject: **DIGITAL TRANSFORMATION AND ARTIFICIAL INTELLIGENCE**

Background and context

In late 2023, the Baltic Defence College (BALTDEFCOL) started a Digital Transformation (DT) and Artificial Intelligence (AI) Working Group (DTAIWG) to implement my vision regarding these topics and to align our education with NATO efforts in this regard.

The initial purpose of the DTAIWG was published in our 2023 Annual Quality Assurance Report to NATO Allied Command Transformation and sent to the Baltic states as an Annex to our Annual Report 2023:

> "Working groups on AI and digital transformation and resilience have been established with first meetings in 2023 and continuing work on deliverables by the end of 2024. The AI and digital transformation working group is investigating two paths. The first path is to continue and expand the education of our students on innovative capabilities and concepts developed to counter or exploit emerging and disruptive technologies to understand their impacts on the character of warfare and how to implement them to ensure our defence and security.'

The initial output of the working group and the pace of advances in artificial intelligence in both military and education contexts make it very clear that the planning horizon has shifted to the right and faster adoption, increased educational content, and budgetary expenditures are necessary.

Mission

BALTDEFCOL will develop staff and students who are appropriately skilled in the innovative, ethical, and secure use of AI and other technological advancements to expand their critical thinking and enhance their performance in the educational and military domains.

Concept

To achieve the mission, the BALTDEFCOL will focus on education, research, tools and capabilities, experimentation, and the collection and dissemination of best practices in the

use of AI and digital tools. Experimentation will be key to this endeavour as the Lessons Learned best practices database does not yet exist, and if it did, it would not be aligned with our unique approach to education.

Research and experimentation in AI/DT by staff and students (with the guidance of faculty) will ensure the responsible use of AI large language models and other technological solutions. Responsible use implies both ethical use and the maintenance of academic integrity.

The use of AI and DT will proceed in agile phases aligned with academic years. The first can best be labelled as experimental partial implementation during AY 2024-2025. Subsequent academic years will see progression to full implementation, currently undefined.

The use of AI in education will be governed by approved policy that is developed and refined in accordance with **Annex A: Baltic Defence College AI Implementation Strategy**.

Tasks and responsibilities

DT/AI Activities will proceed on the following lines of effort in accordance with general regulations and normal standing operating procedures, highlighted in Annex B: Digital Transformation and AI Activities.

- **Working Group Activities and Coordination** (Director DLMS). Manage the DTAIWG on behalf of the CMG, and keep CMG informed of working group activities.

- **Working Group Members** (COS, Department Directors). Ensure that appropriate personnel are contributing to DT/AI activities, including DTAIWG members and other staff exploring and experimenting with technology (including AI) to collect Lessons Learned and best practices to inform educational content and command policies and activities across all lines of effort.

- **Academic Activities** (Dean, Course Directors, Department Directors). Ensure appropriate AI/DT topics are incorporated and integrated into education, including research activities, conferences and roundtables, in accordance with applicable standard operating procedures. Consider the impact of AI tools on assessment processes and adjust if required.

- **Publications** (Dean, Course Directors, Department Directors). Ensure applicable faculty and course participants are conducting research and publication on AI/DT topics.

- **Staff Development** (Dean, Department Directors). Ensure appropriate Staff Development and Professional Development to support DT/AI efforts.

- **IT Support** (Director DOS). Assist in the procurement and integration of applicable IT tools to support DT/AI efforts.

- **ALL.** Tasks and responsibilities as delineated in BALTDEFCOL's internal Regulations.

Administration

1. **Finances and Budget.** Budget holders will consider funding AI/DT activities within applicable preexisting funding lines (e.g.: IT, Staff Development, Professional Development, Education, etc.). It is estimated that initial additional unfunded budget requirements will be limited to AI tool subscriptions (generally 20-30 euros per month per user):

Fiscal Year (FY)	Months	Staff Licences	Syndicate Licences	Total Licences	Cost EUR
FY 2024					
AY 2024-2025	5	28	7	35	4375
FY 2025					
AY 2024-2025	6	28	7	35	5250
AY 2025-2026	6	38	7	45	6750

2. Changes to this guidance, planned activities, and budget will be proposed and amended as required in accordance with internal rules.

3. Amplifying instructions will be issued as required.

/digitally signed/

Annexes:
Annex A: Baltic Defence College AI Implementation Strategy
Annex B: Digital Transformation and AI Related Activities

Annex A
Baltic Defence College AI Implementation Strategy

Baltic Defence College AI Integration Strategy

1. Summary

This strategy outlines BALTDEFCOL's approach to implementing Artificial Intelligence (AI) technologies, ensuring alignment with NATO efforts and our mission in professional military education. It emphasizes ethical considerations, phased implementation, and continuous improvement to enhance our educational capabilities.

2. Purpose and Scope

2.1 Purpose: To guide the responsible development, integration, and use of AI technologies within BALTDEFCOL.

2.2 Scope: Encompasses all AI-related activities at BALTDEFCOL across all lines of efforts, including education, research, development, integration, and use by staff, students, and partners to become a regional hub for incorporating AI in defence.

3. Guiding Principles

3.1 Ethical and Responsible Use: Ensure AI technologies are used ethically, transparently, and accountably in accordance with BALTDEFCOL Regulations and applicable national laws.

3.2 Security and Privacy: Comply with EU and Estonian data protection laws, implementing robust security measures.

3.3 Human-Centric Approach: AI systems should enhance human capabilities, not replace it.

3.4 NATO Alignment: Ensure AI activities support NATO AI efforts.

4. Implementation Strategy

4.1 Phased Approach
- Phase 1 (Experimental (AY 2024-2025)): Select and integrate initial AI tools, focusing on experimentation and learning opportunities.
- Phase 2 (Integration (AY 2025-2026)): Broaden AI integration based on Lessons Learned, scaling successful applications.

4.2 AI Tool Selection and Integration
- Recommended by Digital Transformation and AI Working Group (DTAIWG) in coordination with Departments.
- Prioritize educational value, integration ease, security, and ethical alignment.

- Future tool selection informed by Lessons Learned/Lessons Identified.

4.3 Educational Integration
- Incorporate AI topics into relevant curricula.
- Develop staff AI capabilities through continuous professional development.

4.4 Management Application
- Implement AI to enhance administrative efficiency and decision support systems.

5. Governance and Oversight

5.1 Digital Transformation and AI Working Group (DTAIWG)
- Advise CMG on AI activities, ensuring strategic alignment and best practice integration, and proposing updates to AI Directives and Policies.

5.2 Decision-making Framework
- Based on gathered experience establish protocols for AI-related decisions, ensuring appropriate human oversight.

5.3 Accountability
- Report on AI implementation progress and impacts in appropriate management forums.
- Individual responsibility for AI-related outcomes in accordance with internal rules.

6. Ethical Considerations and Risk Management

6.1 Ethical Framework
- Ensure AI technologies are used ethically, transparently, and accountably in accordance with BALTDEFCOL Regulations and applicable national laws and guided by NATO's policy on responsible use.

6.2 Monitoring and Response
- Monitor and assess the suitability of and, if necessary, amend the internal rules for addressing AI-related incidents or ethical concerns.

6.3 Training and Awareness
- Conduct AI ethics training for all staff and students.

7. Data Privacy and Security

Comply with relevant data protection laws and BALTDEFCOL's internal rules.

Annex A
Baltic Defence College AI Implementation Strategy

8. Continuous Improvement and Evaluation

8.1 Feedback Mechanisms

- Staff and students will provide feedback on AI implementation in accordance with established Quality Management Procedures, After Action Reviews, and Lessons Learned / Lessons Identified mechanisms.

8.2 Review Process

- Conduct annual reviews of AI implementation progress and strategy effectiveness as part of the End of Year Academic Review.

8.3 Performance Metrics

- Identify, develop and track key performance indicators (KPI) for AI implementation.

9. Collaboration and Partnerships

Foster collaborations with NATO educational institutions and relevant organizations to share best practices and advance AI in military education.

10. Strategy Review and Update

This strategy will be reviewed annually (as part of the End of Academic Year Review) by the DTAIWG and updated to reflect technological advancements, changes in NATO guidelines, and implementation of Lessons Learned.

Annex B:
AI/DT Activities

AI/DT Activities

DATE	Key Activities and Deliverables
AUG 24	Develop AY 2024-2025 AI/DT Guidance for Staff
AUG 24	Develop AY 2024-2025 AI/DT Guidance to students
AUG 24	AI/DT Staff Development
AUG 24	Introduce AI Guidance to students
As required	DTAIWG Meeting (collect Lessons Learned, best practices)
SEP 24	Research/Publication (iaw Personal Publication Plans)
SEP 24	Professional Development (iaw Professional Development Plans)
SEP 24	HCSC 2025 CDW
As required	Use Experiment with AI. Professional LLM, Research AI: DTAIWG, Syndicate Computers (7), Library, others as desired. All Others Microsoft Copilot.
As required	AI/DT Staff Development (monthly placeholder to include IT contribution to DT)
As required	Student Education (iaw Course Plans)
DEC 24	IT investigate institutional AI solutions, hardware suitability, budgetary implications
JAN 25	Inputs of DTAIWG to Annual QA Report
TBC	JCDW
TBC	JCGSC CDW
TBC	CSELC CDW
JUN 25	End of AY 2024-2025 Review
AUG 25	Develop AY 2025-2026 AI/DT Guidance for Staff
AUG 25	Develop AY 2025-2026 AI/DT Guidance to students
AUG 25	AI/DT Staff Development (monthly placeholder to include IT contribution to DT)
AUG 25	Introduce AI Guidance to students
As required	DTAIWG Meeting (collect Lessons Learned, best practices)

Annex B:
AI/DT Activities

DATE	Key Activities and Deliverables
SEP 25	Research/Publication (iaw Personal Publication Plans)
SEP 25	Professional Development (iaw Professional Development Plans)
SEP 25	HCSC CDW
As required	Use Experiment with AI. Professional LLM, Research AI: DTAIWG, Syndicate Computers, Library, others as desired. All Others Microsoft Copilot.
As required	AI/DT Staff Development
As required	Student Education (iaw Course Plans)
TBC	JCDW
TBC	JCGSC CDW
TBC	CSELC CDW
JUN 26	End of AY 2025-2026 Review

Policy on the use of Artificial Intelligence in educational activities

This policy addresses the use of any Artificial Intelligence (AI) tools in support of the BALTDEFCOL's educational activities.

The BALTDEFCOL encourages the use of modern approaches and technology, including generative AI, to support teaching and learning. At the same time, genuine achievement of learning objectives must be ensured, and opportunities for academic misconduct minimized. This requires the application of certain precautions and the provision of specific guidance regarding the use of AI in its educational activities.

1. The use of generative AI can enhance the achievement of learning outcomes, expand critical thinking, and assist with speeding up the research process. AI also has some limitations, so it is important to assess its responses critically and verify information with the original source material.

2. Generative AI can be useful in an educational context as an advisor, for example (not all inclusive):

- When doing independent work, to get explanations of concepts, find ideas, improve text, or ask self-check questions.
- To overcome writer's block or the so-called fear of the blank page.
- As a brainstorming assistant.
- As a programming aid.
- For translating texts.
- For developing critical thinking by evaluating its responses to queries.
- To get a general overview of a large amount of material (summarizing texts, data).
- To evaluate or assess a draft work and ask for recommendations on how to improve it.

3. Staff and guest speakers are encouraged to use AI tools (including generative AI chatbots such as OpenAI's ChatGPT and Microsoft's Copilot) in the preparation and delivery of educational activities. This use of AI must be responsible, ethical, transparent, and in support of said educational activities.

4. When preparing an educational activity (i.e., a Module, Elective Module, lecture, syndicate activity, etc.) the person delivering or responsible for the activity must explicitly authorise to what extent, if any, the use of AI is permitted for students. This authorisation requires a clear statement both on ILIAS (if used for the educational activity) and in the text of the assignment. Oral authorisation is also acceptable, but not preferred due to the challenge of later verification. Such oral directions should be documented in writing via the appropriate channel (ILIAS, Microsoft Teams, e-mail, etc.) at the earliest convenience.

5. The use of commonly used tools with task-specific AI elements, such as Grammarly for language editing purposes or web-based search engines for searching information is authorised unless specifically prohibited by the person who has given the assignment.

6. The user shall appropriately declare the use of AI to support completing an assignment. This can be done by either citing the use of AI in written papers or by declaring it in other ways in case of other types of assignments. Generative AI must always be utilized in an ethical fashion, supplementing and supporting the learning process and not replacing the independent thought or work of the individual.

7. Unauthorised use of AI tools or tools with AI elements may be considered academic misconduct and subject to relevant consequences (see Section 4.3.1 of BALTDEFCOL Regulations). Examples of unauthorized use include:

- Having AI complete all of an individual or group task that have been assigned to a person or group.
- Claiming text or content generated by AI as representing original individual or group work without attribution.
- Failure to properly cite or acknowledge the use of AI in the generation of content.

8. The users of AI tools need to recognise the potential that information shared with AI will become available to all users of respective AI tool, therefore it is possible that sharing information with an AI means relinquishing control over the information. Data is protected in conversations with Microsoft Copilot while logged into a person's BALTDEFCOL account (indicated by the green shield). With other AI tools, one should ensure that he/she understands the applicable data protection and privacy policies when sharing information to safeguard sensitive personal and professional data.

9. Entry of personal data into an AI chatbot is prohibited without a person's consent. It is also prohibited to share information with an AI tool that has been restricted for BALTDEFCOL internal, personal, or exercise (faculty) use only (see Section 5.1.2 of BALTDEFCOL Regulations) or classified by NATO or the EU.

10. BALTDEFCOL e-mail addresses can be used to register and/or authenticate oneself for an AI tool. Any use of AI tools in support of BALTDEFCOL's educational activities must be responsible and avoid causing harm to BALTDEFCOL in accordance with this policy.

References

Altair. (2025). *Altair signs MoU with Korea Military Academy to advance AI innovation in defense: Altair to accelerate defense innovation and digital transformation with cutting-edge AI and simulation solutions*. https://altair.com/newsroom/news-releases/altair-signs-mou-with-korea-military-academy-to-advance-ai-innovation-in-defense

Barry, W., & Wilcox, A. B. (2024, October 17). *Hybrid intelligence: Decision dominance at the strategic level*. U.S. Army War College War Room. https://warroom.armywarcollege.edu/articles/hybrid-intelligence/

Chen, L., Chen, P., & Lin, Z. (2020). Artificial intelligence in education: A review. *IEEE Access, 8*, 75264–75278. https://doi.org/10.1109/ACCESS.2020.2988510

European Commission. (2022). *Ethical guidelines on the use of artificial intelligence (AI) and data in teaching and learning for educators*. European Union.

Harvard Business School Publishing. (2024). *How generative AI is reshaping education*. HBP Education's Must Reads. https://bpb-us-w2.wpmucdn.com/hawksites.newpaltz.edu/dist/7/800/files/2024/06/HBP-Education-Must-Reads-How-Generative-AI-is-Reshaping-Education.pdf

Lan, M., & Zhou, X. (2025). A qualitative systematic review on AI empowered self-regulated learning in higher education. *NPJ Science of Learning, 10*, Article 123. https://pubmed.ncbi.nlm.nih.gov/40319057/

Lepik-Verliin, K., Hint, H., & Leijen, D. (2025). AI competence frameworks and policies in higher education: Analysis and recommendations. In *Fostering learners' AI readiness: National report – Estonia*. University of Tartu. https://www.wu.ac.at/fileadmin/wu/o/wu4juniors/LLE/FLAIR/National_Report_Estonia.pdf

Martin, F., & Xie, K. (2022). Digital transformation in higher education: 7 areas for enhancing digital learning. *EDUCAUSE Review*. https://er.educause.edu/articles/2022/9/digital-transformation-in-higher-education-7-areas-for-enhancing-digital-learning

Miao, F., with Giannini, S., & Holmes, W. (2023). *Guidance for generative AI in education and research*. UNESCO.

Mollick, E. (2024). *Co-intelligence: Living and working with AI*. Portfolio/Penguin.

NATO. (2021). *NATO 2030 factsheet*. NATO. Retrieved September 3, 2024, from https://www.nato.int/nato2030/

NATO. (2021). *Summary of the NATO artificial intelligence strategy*. NATO. Retrieved September 3, 2024, from https://www.nato.int/cps/en/natohq/official_texts_187617.htm

NATO. (2022). *NATO 2022 strategic concept*. NATO. Retrieved September 3, 2024, from https://www.nato.int/cps/en/natohq/topics_56626.htm

NATO. (2024). *Emerging and disruptive technologies*. NATO. Retrieved September 3, 2024, from https://www.nato.int/cps/en/natohq/topics_184303.htm

NATO ACT. (2021). *NATO warfighting capstone concept*. NATO Allied Command Transformation. Retrieved September 3, 2024, from https://www.act.nato.int/wp-content/uploads/2023/06/NWCC-Glossy-18-MAY.pdf

NATO ACT. (2023). *Digital transformation*. NATO Allied Command Transformation. Retrieved September 3, 2024, from https://www.act.nato.int/activities/digital-transformation/

NATO Defense College. (2024). *The NATO Defense College launches innovative multi-domain deterrence simulation*. NATO Defence College. https://www.ndc.nato.int/news/news.php?icode=1984&lang=fr&

NATO STO. (2023). *Science & technology trends 2023–2043, across physical, biological, and information domains, Volume 1: Overview*. NATO Science and Technology Organization. https://www.nato.int/nato_static_fl2014/assets/pdf/2023/3/pdf/stt23-vol1.pdf

Shannon, C. E., & Weaver, W. (1959). *The mathematical theory of communication*. University of Illinois Press.

University of Oxford. (2024). *Advice on using artificial intelligence (AI) tools to support your learning*. https://www.ox.ac.uk/students/news/2024-01-08-advice-using-artificial-intelligence-ai-tools-support-your-learning

University of Oxford Centre for Teaching and Learning. (2023). *AI and academic practice*. https://www.ctl.ox.ac.uk/ai

University of Tartu. (2023). *University of Tartu guidelines for using AI chatbots for teaching and studies | Tartu Ülikool*. https://ut.ee/et/sisu/university-tartu-guidelines-using-ai-chatbots-teaching-and-studies

Vial, G. (2019). Understanding digital transformation: A review and a research agenda. *The Journal of Strategic Information Systems, 28*(2), 118–144. https://doi.org/10.1016/j.jsis.2019.01.003

Chapter 20: Before 'Skynet': Cultivating Digital Phronesis in Canadian Military Professional Development Programs

Anne Reiffenstein, ORCID: https://orcid.org/0000-0003-0496-6278

Abstract:

As militaries adapt to an increasingly digital battlespace, leaders face not only technological complexity but also challenges to leadership and ethics. I argue that cultivating digital phronêsis—a form of practical wisdom for the digital age—is essential to preserving human judgment in military decision-making. Drawing on my doctoral research, I propose a construct of digital phronêsis composed of three interdependent domains: digital acumen, digital leadership, and digital ethics. I also propose using a concept analysis methodology for future research and curriculum design in Professional Military Education (PME). Ultimately, I suggest that digital phronêsis is a critical competency for military leaders navigating the ethical and operational demands of an increasingly automated defence environment.

Keywords: Digital phronêsis, military leadership, artificial intelligence, professional military education, digital ethics, human-machine interaction, virtue ethics

Introduction

> *"The Skynet Funding Bill is passed. The system goes online on August 4th, 1997. Human decisions are removed from strategic defence. Skynet begins to learn at a geometric rate. It becomes self-aware at 2:14 a.m., August 29th."*
> *— The Terminator (1984)*

In James Cameron's (1984) original *Terminator* film, a key moment describes how Skynet, an Artificial Intelligence [AI] defence system, becomes *self-aware* and promptly decides that humanity is the threat. Though science fiction, the metaphor rings true as military organizations grapple with the accelerating digitization of the battlespace. While militaries are not yet facing Skynet, they face the ethical and leadership challenges of increasingly autonomous systems, opaque algorithms, and digitally mediated decision-making (Ryan, 2018; Scharre & Horowitz, 2015). This chapter argues that cultivating *digital phronesis* is essential to ensuring that human judgment remains at the heart of military professionalism. In this chapter, I will argue that digitization is changing warfare and digitization is altering the role of humans in decision-making. I will then provide a definition of digital phronesis based on the research I have conducted to date and finally an overview of possible future research could explore.

Warfighting and the digital age

There has long been controversy surrounding the use of machines in warfighting. As early as the 11th century, Pope Innocent III banned the use of the crossbow, arguing that its ease of use and battlefield lethality eroded traditional military hierarchies by allowing commoners to challenge the aristocracy (van der Veen, 2012). Technological innovation has changed the character of warfare throughout history, often with militaries responding only reluctantly. Cavalry charges, for example, persisted well beyond their tactical utility, even after the introduction of tanks in World War I (Zweibelson, 2023).

Today, the Canadian Armed Forces [CAF] acknowledges the necessity of adapting to the digital age (National Defence, 2022). While various strategies have been proposed for procuring technology-enabled warfighting platforms, the human dimensions of this transformation remain underdeveloped. Even the United States—with the largest defence expenditures in the world—has raised concerns about its lack of skilled leadership in the cyber domain. Recent reports indicate that the U.S. Cyber Force is suffering from a shortage of leaders with the expertise required to make critical decisions in cyber operations (Lonergon & Montgomery, 2024; Statista, 2022).

As machines grow more sophisticated and increasingly capable of autonomous action, military leaders at all levels must be equipped to assess and respond to the *digital value proposition* embedded in each decision. These decisions may be institutional—such as determining how much autonomy is permitted in targeting systems—or operational, involving deploying autonomous robotics to achieve mission objectives with minimal harm to military personnel and civilians. The Canadian military is in the midst of a digital transformation, yet its professional development [PD] efforts have only briefly acknowledged the importance of digital literacy (National Defence, 2022). Within the CAF, digital literacy frameworks are primarily imported from civilian contexts, such as the Skills Framework for the Information Age [SFIA] (2023). As explained by Bill Railer, Director of the Canadian Advanced Distributed Learning Lab and the CAF's lead for education technology, SFIA emphasizes technological fluency—an understanding of "the machine" in the human-machine interface (B. Railer, personal communication, August 30, 2023; SFIA, 2023).

However, the CAF's PD system has yet to address how military leadership itself is evolving in the digital era. Research on digital leadership is still nascent, even in civilian sectors, and there is no universally accepted definition (Cortellazzo et al., 2019; Wang, 2022). As a result, the CAF has not yet articulated the competencies required of a digital military leader, making it difficult to determine the education and training needed for their development. The CAF's PD doctrine aims to "prepare members intellectually and professionally to meet the anticipated challenges in the ambiguous, chaotic and complex security environment" (National Defence, 2018, para. 2). Yet, the most recent syllabi from Canadian military education

institutions make no mention of digitization (National Defence, 2019a; National Defence, 2019b). To lead effectively in this evolving context, Canadian military leaders must be prepared to confront and evaluate digital propositions—be they institutional or operational. Doing so requires more than technical knowledge; it demands practical digital wisdom. This chapter adopts Aristotle's concept of *phronêsis*, reinterpreted for the digital age. Following Kristjánsson et al. (2021) definition of *phronêsis* is defined here as "an intellectual meta-virtue, adjudicating the courses of action recommended by various moral virtues through integrative, holistic, critical metacognition" (p. 244).

Digital phronêsis centers the human element within the human-machine interface. It offers a framework for cultivating ethical, wise, and context-aware decision-making—capabilities critical for future military leaders navigating increasingly autonomous and complex technological systems. Before examining the proposed construct for digital phronesis, a brief overview of some of the theoretical concepts may be helpful.

Theoretical and Practical Foundations of Digital Phronesis

Aristotle originally proposed *phronêsis*—often translated as practical wisdom—as the intellectual virtue most essential for achieving *eudaimonia*, or human flourishing. It is the ability to make sound, ethical decisions in complex, real-world situations, drawing on experience and guided by moral character (Aristotle et al., 2014). As a core component of virtue ethics, *phronêsis* emphasizes not only knowing what is good, but acting on it with sound judgment in context.

Although virtue ethics declined in prominence during the rise of deontological and consequentialist moral philosophies, it has experienced a resurgence in both business and military ethics, where character is increasingly recognized as critical to effective leadership (Crossan, 2021; Hursthouse et al., 2022; National Defence, 2022; Snow, 2018). Annas (2007) emphasized that practical reasoning lies at the heart of virtue ethics; according to Snow (2018), virtue is a disposition to act in certain ways based on such reasoning. This aligns with the CAF Ethos, which promotes character as equally important as competence and articulates values, principles, and professional expectations that suggest an implicit commitment to virtue ethics (National Defence, 2022).

However, while the CAF doctrine draws heavily on the language of character, it notably omits any reference to *phronêsis*, practical wisdom, or even wisdom more broadly. In discussions with the authors of the CAF Ethos, it became clear that concerns about accessibility and readability played a role in this omission (W. Cummings & G. Martinelli, personal communication, 26 May 2022). This hesitation may reflect a broader critique of classical virtue ethics, as Annas (2007) noted, which is sometimes perceived as overly academic or elitist.

More recent scholarship has pushed back against that critique. Kristjánsson et al. (2014) argued that *phronêsis* is particularly suited to professions involving human judgment and ethical complexity, proposing it as a way to rescue professional ethics from "the clutches of a stale rule and code-fetishizing formalism" (p. 154). Shotter and Tsoukas (2014) highlighted *phronêsis* as the cornerstone of wise leadership, describing "phronetic practitioners" as those with a refined capacity to intuitively grasp the most salient features of ambiguous situations (p. 381). Nonaka and Takeuchi (2021) offer a complementary organizational perspective, framing *phronêsis* as a product of collective learning that emerges when individual actions harmonize through the Socialization-Externalization-Combination-Internalization [SECI] model. Together, these contemporary interpretations support the view that *phronêsis* is relevant and urgently needed in the military domain—especially in digitally complex environments. Yet, despite its clear applicability, *phronêsis* remains absent from military doctrine and PD programs in the CAF.

AI and automation increasingly threaten to displace the low-stakes decision-making essential for developing tacit knowledge in leaders. These routine, everyday judgments—what might be considered the mundane "chores" of leadership—are foundational for building practical wisdom. They offer opportunities to practice judgment, adapt to evolving contexts, and develop a nuanced understanding of organizational dynamics. As automation absorbs these tasks, there is a risk that future leaders will be denied the very experiences that cultivate confidence, critical thinking, and ethical discernment. Shannon Vallor (2015) describes this phenomenon as *moral deskilling*: a process through which overreliance on machines erodes human moral capacity by displacing the conditions under which moral skills are learned and practiced. Like the *Sorcerer's Apprentice*, who delegates his duties to enchanted brooms only to lose control of the consequences, military leaders who offload foundational decision-making to algorithms may find themselves similarly unprepared when automation exceeds their understanding or intent (Disney, 1940; Harari, 2024). Without regular, low-risk opportunities to refine their judgment, military professionals risk entering complex operational environments unequipped to make decisions that are not only technically sound, but morally wise.

What is Digital Phronesis? A Construct for Military Professional

There is no agreed definition for the term digital phronesis. In some research, it has been used to describe preparing school children for their lives in a digital world (Krisjanesen, 2014), or it has been more as a function to join together a digital morality that would be accepted globally (Ess, 2020). However, as a goal or an outcome to be achieved, it has not been examined to determine its domain. From my research, I have proposed an initial construct built of three interdependent domains: Digital Acumen, Digital leadership and Digital Ethics for military leaders.

Digital Acumen

Digital acumen is a term that intends to capture the behaviours, attitudes and skills that are required to operate in a digital environment (Tosczak, 2023). These encompass an openness or acceptance of technology digital literacy (National Defence, 2023), which is situational fluency in the technical requirements of a particular position or occupation (National Defence, 2023; Venkatesh et al., 2016). This technical fluency allows decision-makers to understand their experts and consider the technical advice critically. There are obstacles to digital acumen, such as math hesitancy, a concept that many adults fear of math and associated technical/science propositions (Kumar & Krishna, 2025; Schiavo et al., 2024). There is some generational disdain for some technology that provides a barrier to learning the language of digital propositions. As such, there is a need to educate, as has been recognized by the CAF with the efforts to establish digital literacy as part of PME (National Defence, 2023). This effort is nascent and does not address the barriers to technology use but instead, it aims to provide digital fluency.

Digital Leadership

Digital leadership, again, is a term used extensively but with wide-ranging meaning ranging from leading a dispersed team using electronic means to leading in a technological age. There is a significant amount of literature related to digital leadership, with several recent examinations of the literature, such as a scoping review, a literature review, and a bibliometric analysis, all completed in the last two years (Cortellazzo et al., 2019; Sağbaş, M. & Erdoğan, F., 2022; Tigre et al., 2023). Digital leadership is seen largely as an extension of existing leadership theory, with the most common referrals to transformational leadership theory and shared leadership. The literature seems to split in its focus with a view on the individual leader development of attributes and skills to perform to adapt to this new leadership environment or there is an organizational focus with digital leadership being viewed with the context of digital transformation of business operations (Eberl & Drews, 2021; Kane et al., 2019; Khaw et al., 2022; Oberer & Erkollar, 2018; Sağbaş & Erdoğan, 2022). However, in the literature that discusses the leading human-machine teams, there is a view that algorithms can make decisions from a rationale perspective better than many humans, and the digital leaders should focus on what uniquely human attributes can be brought to the question of leadership (De McGuire & De Cremmer, 2023; Logg et al., 2019). These can include visionary thinking, culture building and influence as well as the soft skills that are required in leading humans, such as the behaviours that reflect empathy, humility, and temperance (Crossan, 2014; McGuire & De Cremmer, 2023; Pierre, 2022).

Digital Ethos

Digital ethics, or techno-morality, forms the third pillar of digital *phronêsis*. It focuses on recognizing, reflecting upon, and acting consistently with core military and democratic values in an increasingly automated, opaque, and information-saturated environment (Vallor, 2016; Ess, 2020). Unlike traditional ethics that emphasizes decision-making in static, human-only environments, digital ethics concerns the shifting social norms, algorithmic mediation, and blurred accountability of digital systems (Vallor, 2016; 2024). As Vallor (2016) argues, digital platforms mediate not just action but perception, slowly establishing new norms about what counts as efficient, effective, or acceptable. This can lead to the tacit acceptance of autonomous decision-making without critical reflection (del Aqua et al., 2023; Logg et al., 2019). Building on the earlier discussion of Vallor's (2016) concept of moral deskilling, digital ethics in the military must recognize that not all threats are kinetic—some are ethical capabilities slowly atrophied by automation. Vallor (2016) warns that when key decisions are handed over to machines, humans may lose the opportunity to learn responsibility for these decisions and their outcomes. A third ethical challenge in digital military environments is the problem of attribution and accountability. As responsibility becomes distributed across human-machine networks, who is held accountable when things go wrong? Elish (2019) introduced the concept of the *moral crumple zone* to describe how responsibility is often pushed onto the nearest human operator—regardless of whether they had real control over the outcome. In military operations, this dynamic could undermine trust and organizational cohesion, as junior personnel may bear the burden of ethical failure caused by complex institutional, technical, or algorithmic decisions made far upstream.

From a legal perspective, accountability can be identified along the lines of civil frameworks like the EU General Data Protection Regulation [GDPR] offer instructive contrasts (Regulation (EU) 2016/679, 2016). Article 22 of the GDPR mandates that individuals have a right not to be subject to automated decision-making without meaningful human oversight and that accountability lies with the originator of the system, not the end user (Regulation (EU) 2016/679, 2016). While military contexts differ from civilian data environments, the principle of *origin-based accountability* could serve as a useful model for developing ethical governance in defence settings. In Canada, the *Directive on Automated Decision-Making* (Treasury Board of Canada Secretariat, 2019) provides a risk-based framework requiring human involvement in high-impact automated decisions. However, it falls short of articulating a clear approach to accountability or attribution in defence applications, highlighting a significant policy gap. Military PD programs must prepare leaders to not only comply with evolving legal frameworks but also to critically assess the ethical architecture of the systems they rely on—and to take meaningful responsibility for the outcomes those systems help produce.

The evolving digital landscape presents both opportunities and challenges for military leadership development. The three domains of Digital Acumen, Digital Leadership, and Digital Ethics together form a foundational construct for digital *phronêsis* in military leaders. As the integration of AI, automation, and digital systems becomes increasingly central to military operations, leaders must cultivate technical expertise and the moral and ethical judgment required to navigate this complex environment.

Next Steps: Research and Application in Military PME

The construct of digital *phronêsis* proposed in this chapter represents a preliminary framework that requires further refinement and validation. The next research phase will focus on concept analysis through case model scenarios and structured data collection from subject matter experts and military professionals. To support the construct analysis of digital *phronêsis*, this study will also employ case model development based on the method proposed by Walker and Avant (Nuopponen, 2010). Originally developed for concept analysis in nursing and health sciences, Walker and Avant's structured approach has been widely adapted for use in social and behavioural research. It provides a systematic way to clarify and refine conceptual definitions through the construction of illustrative cases.

With this methodology, the case model scenarios will serve two purposes: to clarify the defining attributes of each domain within the digital *phronêsis* construct—digital acumen, digital leadership, and digital ethics and to guide and ground the semi-structured interview process with subject matter experts and military practitioners.

Following Walker and Avant's methodology, each domain will be explored through four key case types: Model case which is a scenario that clearly exemplifies the concept in its entirety, including all critical attributes; A borderline case, a scenario that contains most but not all defining features, highlighting ambiguities in application; a related case outlining a scenario that is connected to the concept but does not represent it directly, helping to delineate conceptual boundaries; and a contrary case, where a scenario that clearly does *not* reflect the concept, used to sharpen understanding of what the concept is not (Nuopponen, 2010). For example, a model case for digital leadership might involve a senior military leader successfully integrating human–machine teaming in a way that enhances mission performance while preserving ethical agency and team cohesion. A contrary case might depict a scenario in which a leader delegates all key decisions to an autonomous system, resulting in an accountability failure and mission breakdown. These scenarios will be refined through expert consultation and will serve as prompts during interviews to stimulate reflection, comparison, and critique. This will ensure that abstract conceptual elements are made concrete, context-specific, and useful for PD purposes.

The goal of this analysis is twofold: first, to inform the development of a curriculum framework for integrating digital *phronêsis* into PME and second, to support the creation of validated assessment tools capable of identifying individual and organizational strengths as well as areas requiring further development. By systematically evaluating how military professionals engage with digital acumen, leadership, and ethical reasoning, the research aims to provide actionable insights that can guide both curriculum design and policy development in the digital age.

Conclusion

Ultimately, cultivating digital *phronêsis* is not only a response to technological change, it is a commitment to preserving the ethical centre of military professionalism in an era when machines are no longer just tools, but actors within the decision space. As we edge closer to environments where autonomous systems influence or even make decisions with life-and-death consequences, the validity of Vallor's (2018; 2024) question where it is no longer whether we can delegate to machines, but whether we should, becomes more important. In the world imagined by *The Terminator*, Skynet's self-awareness marked the moment when humanity lost control of its creation (Cameron, 1984). In our reality, it is not self-aware machines we must fear, but the gradual erosion of human judgment, responsibility, and wisdom in the face of seductive automation. Digital phronêsis is what ensures that military leaders remain not just operators of advanced systems, but stewards of human values within them.

References

Annas, J. (2007). *Virtue Ethics*. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780195325911.003.0019

Aristotle, Barnes, J., & Kenny, A. (2014). *Aristotle's Ethics: Writings from the Complete Works - Revised Edition*. Princeton University Press. http://ebookcentral.proquest.com/lib/royalroads-ebooks/detail.action?docID=1689364

Cameron, J. (Director). (1984). *The Terminator* [Video recording]. Orion Pictures.

Cortellazzo, L., Bruni, E., & Zampieri, R. (2019). The role of leadership in a digitalized world: A review. *Frontiers in Psychology*, *10*, 1938. https://doi.org/10.3389/fpsyg.2019.01938

Crossan, M., Côté, S., & Virgin, S. (2021). Elevating leader character alongside competence in selection. *Organizational Dynamics*, *50*(3), 100752. https://doi.org/10.1016/j.orgdyn.2020.100752

Dell'Acqua, F., McFowland, E., Mollick, E. R., Lifshitz-Assaf, H., Kellogg, K., Rajendran, S., Krayer, L., Candelon, F., & Lakhani, K. R. (2023). Navigating the jagged technological frontier: Field experimental evidence of the effects of AI on knowledge worker productivity and quality. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4573321

Disney, W. (Director). (1940). Fantasia [Film]. Walt Disney Productions.

Eberl, J., & Drews, P. (2021). *Digital leadership – mountain or molehill? A literature review* (pp. 223–237). https://doi.org/10.1007/978-3-030-86800-0_17

Elish, M. C. (2019). Moral Crumple Zones: Cautionary Tales in Human-Robot Interaction. *Engaging Science, Technology, and Society*, *5*, 40–60. https://doi.org/10.17351/ests2019.260
Ess, C. M. (2020). Interpretative Pros Hen Pluralism: From Computer-Mediated Colonization to a Pluralistic Intercultural Digital Ethics. *Philosophy & Technology*, *33*(4), 551–569. https://doi.org/10.1007/s13347-020-00412-9
Harari, Yuval N., Nexus: A Brief History of Information Networks From the Stone Age to AI. Random House, 2024.
Hursthouse, R., & Pettigrove, G. (2023). Virtue Ethics. In E. N. Zalta & U. Nodelman (Eds.), *The Stanford Encyclopedia of Philosophy* (Fall 2023). Metaphysics Research Lab, Stanford University. https://plato.stanford.edu/archives/fall2023/entries/ethics-virtue/
Kane, G. C., Phillips, A. N., Copulsky, J., & Andrus, G. (2019). How Digital Leadership Is(n't) Different. *MIT Sloan Management Review*, *Spring*.
Khaw, T. Y., Teoh, A. P., Abdul Khalid, S. N., & Letchmunan, S. (2022). The impact of digital leadership on sustainable performance: A systematic literature review. *Journal of Management Development*, *41*(9/10), 514–534. https://doi.org/10.1108/JMD-03-2022-0070
Kristjánsson, K. (2014). Phronesis and moral education: Treading beyond the truisms. *Theory and Research in Education*, *12*(2), 151–171. https://doi.org/10.1177/1477878514530244
Kristjánsson, K., Fowers, B., Darnell, C., & Pollard, D. (2021). Phronesis: Practical wisdom) as a type of contextual integrative thinking. *Review of General Psychology*, *25*(3), 239–257. https://doi.org/10.1177/10892680211023063
Logg, J. M., Minson, J. A., & Moore, D. A. (2019). Algorithm appreciation: People prefer algorithmic to human judgment. *Organizational Behavior and Human Decision Processes*, *151*, 90–103. https://doi.org/10.1016/j.obhdp.2018.12.005
Lonergan, E. & Montgomery, M. (2024). *United States cyber force: A defense imperative*. Foundations for Defence of Democracies. https://www.fdd.org/analysis/2024/03/25/united-states-cyber-force/
McGuire, J., & De Cremer, D. (2023). Algorithms, leadership, and morality: Why a mere human effect drives the preference for human over algorithmic leadership. *AI and Ethics*, *3*(2), 601–618. https://doi.org/10.1007/s43681-022-00192-2
Nonaka, I., & Takeuchi, H. (2021). Humanizing strategy. *Long Range Planning*, *54*(4), 102070. https://doi.org/10.1016/j.lrp.2021.102070
National Defence, G. of Canada. (2018, December 13). *Canadian Armed Forces professional development framework* [Education and awareness]. https://www.canada.ca/en/department-national-defence/services/benefits-military/education-training/professional-development/framework.html
National Defence, G. of Canada. (2019a). *Syllabus: Canadian Forces College joint command and staff programme residential).* Syllabus: Canadian Forces College Joint Command and Staff Programme Residential. https://www.cfc.forces.gc.ca/118/406/cfc300-46-eng.pdf
National Defence, G. of Canada. (2019b). *Syllabus: Canadian Forces College national security programme (NSP)*. Syllabus: Canadian Forces College National Security Programme. https://www.cfc.forces.gc.ca/119/187/324/331-eng.pdf
National Defence, G. of Canada. (2022, June 10). *Canadian Armed Forces Ethos: Trusted to Serve*. https://www.canada.ca/en/department-national-defence/corporate/reports-publications/canadian-armed-forces-ethos-trusted-to-serve.html
National Defence, G. of Canada. (2023, February 28). *Canadian Armed Forces Digital Campaign Plan*. https://www.canada.ca/en/department-national-defence/corporate/reports-publications/canadian-armed-forces-digital-campaign-plan.html
Nuopponen, A. (2010). Methods of concept analysis – a comparative study. *Language for Special Purpose*, *1*(1).

Oberer, B., & Erkollar, A. (2018). Leadership 4.0: Digital leaders in the age of industry 4.0. *International Journal of Organizational Leadership*, *7*(4), 404–412. https://doi.org/10.33844/ijol.2018.60332

Pierre, A. (2022). *Leadership of Human-Machine Teams in Military Environments: An Exploratory Framework*. Regent University.

Regulation (EU) 2016/679. (2016, April 27). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. Official Journal of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

Ryan, M. (2018). *Human machine teaming for future ground forces*. Centre for Strategic and Budgetary Assessment.

Sağbaş, M. & Erdoğan, F. (2022). *Digital leadership: A systematic conceptual literature review*. https://dergipark.org.tr/en/download/article-file/2083776

Scharre, P. & Horowitz, M. (2015). *An introduction to autonomy in weapon systems* [Working Paper]. Center for New American Security.

Schiavo, G., Businaro, S., & Zancanaro, M. (2024). Comprehension, apprehension, and acceptance: Understanding the influence of literacy and anxiety on acceptance of artificial Intelligence. *Technology in Society*, *77*, 102537. https://doi.org/10.1016/j.techsoc.2024.102537

SFIA Foundation. (n.d.). *Skills framework for the information age* [Menu]. SFIA. Retrieved June 17, 2023, from https://sfia-online.org/en/sfia-8/sfia-views/full-framework-view

Shotter, J., & Tsoukas, H. (2014). In Search of *Phronesis*: Leadership and the Art of Judgment. *Academy of Management Learning & Education*, *13*(2), 224–243. https://doi.org/10.5465/amle.2013.0201

Snow, N. E. (2018). *The Oxford handbook of virtue*. Oxford University Press.

Statista. (2022). *Military spending by country worldwide 2022*. Statista. https://www.statista.com/statistics/262742/countries-with-the-highest-military-spending/

Tigre, F. B., Curado, C., & Henriques, P. L. (2023). Digital Leadership: A Bibliometric Analysis. *Journal of Leadership & Organizational Studies*, *30*(1), 40–70. https://doi.org/10.1177/15480518221123132

Tosczak, M. (2023). How to increase your students' digital acumen. *Journal of Accountancy*. https://www.journalofaccountancy.com/newsletters/academic-update/how-to-increase-your-students-digital-acumen/

Treasury Board of Canada Secretariat. (2019). *Directive on automated decision-making*. Government of Canada. https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/automated-decision-making.html

Vallor, S. (2015). Moral Deskilling and Upskilling in a New Machine Age: Reflections on the Ambiguous Future of Character. *Philosophy & Technology*, *28*(1), 107–124. https://doi.org/10.1007/s13347-014-0156-9

Vallor, S. (2016). *Technology and the Virtues: A Philosophical Guide to a Future Worth Wanting*. Oxford University Press.

Vallor, S. (2024) *The AI mirror*: *How to reclaim our humanity in the age of machine thinking.* Oxford University Press.

Venkatesh, V., Thong, J., Hong Kong University of Science and Technology, Xu, X., & The Hong Kong Polytechnic University. (2016). Unified Theory of Acceptance and Use of Technology: A Synthesis and the Road Ahead. *Journal of the Association for Information Systems*, *17*(5), 328–376. https://doi.org/10.17705/1jais.00428

van der Veen, V. (2012). Crossbows and christians: The church's ban of the crossbow. *Medieval Warfare*, *2*(2), 38–41. https://www.jstor.org/stable/48577944.

Wang, T., Lin, X., & Sheng, F. (2022). Digital leadership and exploratory innovation: From the dual perspectives of strategic orientation and organizational culture. *Frontiers in Psychology*, *13*, 902693. https://doi.org/10.3389/fpsyg.2022.902693

Zweibelson, B. (2023). Part i: The singleton paradox: on the future of human-machine teaming and potential disruption of war itself. *Journal of Advanced Military Studies*, *14*(1), 11–46. https://doi.org/10.21140/mcuj.20231401001

Section 4: Fostering Public-Private Cooperation

Chapter 21: Military Capability Development in Europe: Considering a Normative Ecosystem Perspective

Lt-Col. Johanna **Jungwallius**, ORCID: https://orcid.org/0009-0007-0359-3277

Abstract:
Despite increasing defence budgets and strong political will across European countries, military capability development still struggles with poorly coordinated planning and missed opportunities for synergy. Diverging interpretations of what 'capability development' entails among decision-makers may further complicate alignment efforts. Addressing the complexity and the interconnected nature of capability development is essential, not only for achieving synergies in research and development, but also for aligning planning processes for defence manufacturers. This discussion paper adopts a holistic perspective on military capability development. It reviews interconnected research fields, including industrial and defence policies, knowledge transfer, the triple helix framework, and cross-sectoral co-creation. Engaging with theory-driven research, the paper discusses both the potential benefits and limitations regarding the utility of a normative ecosystem model to provide concrete guidance for decision-makers. While acknowledging the challenges of applying such a model, it argues that the model supports a more integrated understanding of military capability development as an interconnected ecosystem. Rather than providing an explanatory account, the paper aims to prompt further reflection on the model's relevance for policy and practice and to promote a broader understanding of the interdependencies of military capability development.

Keywords: military capability development, defence-industrial collaboration, Triple Helix, co-creation, normative models

Introduction

Diverging perspectives between policymakers and military end-users on what constitutes 'capability development' risk undermining communication, cooperation, and the identification of synergies within defence planning processes (Giry & Smith, 2019). These misalignments - exacerbated by cultural and institutional differences and competing priorities - can have concrete strategic consequences. Russia's invasion of Ukraine has made this acutely clear: European countries are struggling to provide munitions and support to Ukraine at the scale and speed required (Caverley, 2023). These concerns coincide with the proposition by the European Union [EU] to strengthen the member states' collective defence industrial efforts (Ostanina & Tardy, 2024). Furthermore, European NATO countries are expected to boost their respective national military capabilities (Clapp, 2024; Faure, 2025; Siebold & Bayer, 2025). These incentives and initiatives may face challenges, as several of

these countries also strive to maintain their defence industry autonomy (Calcara & Simón, 2024; Mueller, 2025). Taken together, this underscores how a fragmented and poorly coordinated approach may counteract common political goals of collaboration within and between European and EU countries, which may lead to increased risks for supply chains and military operations (Faure, 2025; Fabbrini, 2025; Mueller, 2025). However, due to the urgency caused by the war in Ukraine, the political momentum for military capability development is strong. Research and technical expertise are flourishing across European industries and research institutes (Liwång, 2022; Ostanina & Tardy, 2024), with increasing emphasis on innovation, co-creation, and cross-sector collaboration. To harness this opportunity and to achieve effective outcomes, coordination and strategic alignment are indispensable. This, in turn, hinges on the ability of policymakers and end-users to transition from stove-piped to interlinked decision-making (Bellais, 2023; Faure, 2025). Thus, a more integrated perspective in decision-making may be required - one that acknowledges foundational interdependencies, manages to coordinate efforts and has the ability to identify both synergies and bottlenecks.

This discussion paper explores key patterns and tensions in research on military capability development, aiming to prompt further reflection on the model's relevance for policy and practice. It engages with theory-driven literature to assess the utility of a normative ecosystem model as a framework for understanding capability development as an interconnected process. The discussion draws on scholarship related to defence industrial policies in Europe, as well as research on normative models, cross-sectoral co-creation, and the triple helix framework, which highlights knowledge-sharing among academia, industry, and government.

The paper defines the ecosystem model as a framework for describing and highlighting interactions among highly complex elements (Tan & Chang, 2008), recognising the model's potential to provide actionable guidance to decision-makers and stakeholders, which means it also reflects on the model's normative capacity that goes beyond its descriptive design (Beck & Jahn, 2020).

The text is organised into three sections. First, it explores European and EU defence industrial policies and collaborative efforts, illustrated by research examples of how military capability development is shaped by national contexts and historical experiences. This section also reflects on scholarly discussions on triple helix and co-creation and discusses possible implications when decision-making is based on divergent understandings of 'capability development'. The following section conceptualises the normative ecosystem model. In its third section, the paper considers the application of the normative 'ecosystem' model to military capability development, linking back to earlier discussions on European defence industrial policy and knowledge transfer. The concluding remarks summarise the discussions and propose further avenues for exploration beyond the aim and scope of this paper.

Military Capability Development across Europe: National Conditions, Scholarly Debates, Conceptual Divergences

This section explores how varying national contexts, and historical trajectories have influenced approaches to - as well as the evolution of - defence capability development among different European NATO countries. The literature illustrates notable divergences among these countries, that present obstacles for military capability development, but also potential areas for synergy and collaboration. To allow for structured reading, the section is divided into three sub-headings: (1) Key conditions for military capability development in European NATO countries; (2) Military capability development through a triple-helix model and co-creation lens; and (3), Diverging conceptualisations of 'capability development'.

Key conditions for military capability development in European NATO countries

National defence industrial bases often play a significant role in shaping international relations, as industrial initiatives are closely tied to their respective governments (Håkansson, 2021). In this context, it is important to consider the shared historical experiences of several Western European countries. Many of their defence industries were initially developed during the Cold War and remain largely shaped by that legacy. Despite rapid technological advancement and a changing geopolitical landscape, these industries have been slow to adapt to new strategic and technological conditions (Wang et al., 2017; Sezal & Giumelli, 2021; Bellais, 2023). The primary objective of domestic defence industries still remains: to maintain a national and self-sufficient defence sector under close governmental oversight (Bellais, 2023). This has led to the dominance of a few, major defence-industrial 'champions', for instance in the aerospace sector (Giry & Smith, 2020; Ditrych & Kucera, 2023). Countries such as Sweden, France and Britain have retained their own 'champions', despite these legacy industries also facing criticism for not being efficient or flexible enough (Giry & Smith, 2020). In part, this criticism is based on these legacy industries being forced to follow ideals of "faster, cheaper, better", keeping industrial efficiency in the political cross-hairs (Giry & Smith, 2020, p. 437). This points to one of the effects of strong underlying relationships between government and industry that shape their respective yet similar path dependencies. What is more, reinforcement of domestic industrial 'champions' continues to shape defence and foreign policymaking in both direct and indirect ways (Yue & Henshaw, 2009; Olsen, 2022; Sezal & Giumelli, 2022; Mueller, 2025). A clear example of direct influence is the co-development of large-scale projects like the Airbus Group, which involves Germany, France, and Spain. Such initiatives require strong political backing domestically as well as bilaterally and could strengthen mutual dependencies among participating states (Ditrych & Kucera, 2022; Mueller, 2025). Indirectly, prioritising these industries contributes to a shared identity

and trust among EU member states (Ditrych & Kucera, 2022). Despite this, many European countries still depend on non-European defence products (Mueller, 2025). Taking these conditions into consideration, it is not surprising that emerging or smaller firms seeking to enter the European defence market face significant barriers, as the landscape is already dominated by well-established players; a dominance further solidified by close government-industry ties and sustained political support (Bellais, 2023).

Another influential factor is the way these countries manage defence equipment procurement, reflected in the institutionalised processes of defence capability planning (Giry & Smith, 2020; Bellais, 2023). This is not only because of the huge costs involved in procuring or manufacturing platforms: defence industrial projects often span multiple policy areas (Giry & Smith, 2020). It is therefore not uncommon for these projects to have an influence beyond the growth of national commercial enterprises, and to shape bilateral defence industry collaborations. Sweden, because of it being a relatively small country, is an illustrative example: with its long history of developing and exporting its own fighter aircraft systems (Swedish Ministry of Defence, 2024), the country is faced with the risk of losing influence in the defence industrial market compared to larger, more dominant global players (Håkansson, 2021). This concern is also transparent in Sweden's strategic policy. For example, in 2023, the Swedish Government launched a defence innovation initiative aimed to reinforce national control over military technologies (Swedish Ministry of Defence, 2024). As for larger European economies, there are other, political concerns shaping conditions that suggest possible obstacles for bilateral collaborations. For example, while France tends to be more hesitant about market integration with other European countries, Germany stands to benefit from such arrangements due to its comparatively stronger commercial technological base (Calcara & Simón, 2024). Given Germany's, but also France's central role in the European economy, these dynamics point to broader implications for European countries: compared to the US, Europe is marked by its fragmented defence industrial market (Mueller, 2025) and their defence industries have remained bureaucratic despite current crises and events. For the United Kingdom [UK] - another major European economy - military capability development was initially a relatively de-politicised process. Over time, however, it has become more administrative. Identifying capability needs and determining how best to meet them is primarily framed as a matter of resource management (Giry & Smith, 2020). This managerialism seems to be a recurring theme for several other European countries, creating similar tensions across Europe, in terms of cost-effectiveness, industrial efficiency and agility (Sezal & Giumelli, 2022; Bellais, 2023; Fabbrini, 2025; Mueller, 2025).

While industry itself cannot deliver military capability, it is nevertheless fundamental for maintaining a country's industrial skills and for providing important military means. Therefore, it is considered problematic if it is not sufficiently defined or understood as part of the equation

in terms of the overall military capability development (Yue & Henshaw, 2009). As capability features at all levels of planning and development of military needs, it is fundamentally contextual in its nature (Yue & Henshaw, 2009). However, while striving for defence industry autonomy may be true for a number of Western European countries, it does not necessarily apply to all. To illustrate this contrast, the Czech and Slovak defence industry domain became fragmented following the collapse of the Soviet Union (Chovančík, 2018; Krpec & Kříž, 2025). Since then, their respective defence-industrial policies have struggled to break away from their past as former Soviet-aligned states (Chovančík, 2018; Krpec & Kříž, 2025). For Slovakia, it resulted in a governmentally controlled industry that focuses on tanks and large-calibre ammunitions (Chovančík, 2018). For the Czech Republic, its capability development has been based on highly specialised equipment, producing, among other things, advanced optics for the global aerospace industry (Krpec & Kříž, 2025). Both countries have sought bilateral initiatives in defence industries since the 1990s, pursuing collaborations with larger firms abroad (Chovančík, 2018; Krpec & Kříž, 2025), but also to pursue collaborative efforts between the two countries (Chovančík, 2018). Military capability development in the Czech Republic and Slovakia is shaped by conditions that differ markedly from those of Western European countries, due to both historical and structural factors. International defence capability collaborations have been at the forefront (Chovančík, 2018), for instance the procurement of the Swedish Gripen fighter aircraft to the Czech Republic (Krpec & Kříž, 2025). At the same time, their larger enterprises have continued to maintain older, Soviet-era systems. The Czech armed forces have therefore struggled to integrate much of the domestically manufactured niche technologies (e.g. advanced passive radar and optics systems) into their defence capabilities and platforms (Krpec & Kříž, 2025). Conversely, Slovakia's defence industry has developed and integrated some of theirs into their domestic capabilities, particularly for its national army. As an example, several of their armoured vehicles can now be fitted with an upgraded tank turret featuring an advanced control system (Chovančík, 2018). Research suggests that the domestic markets of similar Central and Eastern European countries reflect a strong emphasis on building on established industrial capacities, potentially overlooking necessary defence development and alignment with Western European defence capabilities (Krpec & Kříž, 2025). In sum, current research underscores a notable gap in military capability development across European NATO countries – both structurally but also reflected in the different countries' defence industrial policies.

While, historically, several defence industries in Europe have developed military capabilities in a rather stove-piped manner, they are now increasingly pursuing partnerships across different sectors (Ditrych & Kucera, 2023). Given the current uncertainties, both in the security landscape, and regarding partnerships and coalitions, it is likely that many European

countries with shared threat perceptions will continue along this path (Ditrych & Kucera, 2023). In a policy brief on strengthening the defence capacity in the EU, the long-term vision of the European Defence Industrial Strategy is described as a means of ensuring a certain degree of autonomy (Ostanina & Tardy, 2024). Despite production capabilities being deemed insufficient within the EU, these initiatives have nevertheless strengthened defence industry collaborations between member states. At the policymaking level, the goal is to establish a unified industrial strategy (Ostanina & Tardy, 2024). The trilateral initiative between France, Germany, and Spain to develop a sixth-generation fighter aircraft exemplifies this shift (Calcara & Simón, 2024). However, projects of this scale are unlikely to be without challenges. The key issue is that such cross-sector, multinational initiatives require a coordinated political, industrial, and financial effort, along with considerations for social and environmental sustainability (Ostanina & Tardy, 2024; Malmio, 2024). This leads into the topic of how these very context-depending and different military capabilities may co-evolve and what this could imply in terms of long-term planning processes (Yue & Henshaw, 2009), but also what synergies this could offer. The examples discussed in this sub-section exemplify different paths among European countries to develop and acquire defence capabilities and their strategic and economic significance. Though this is valuable research, it may overshadow other essential aspects of military capability development across Europe, such as emerging technologies in artificial intelligence [AI] for the defence sector (Caverley, 2023).

Military capability development through a triple-helix model and co-creation lens

Importantly, military capability development is not an activity restricted to governmentally controlled defence industries or private profit-seeking firms alone. Scholarly interest in knowledge-transfer and collaborative potential between academia, industry and government has expanded in recent years (Liwång, 2022; Liwång et al., 2023; Malmio, 2024; Schebesch, Soim & Blaga, 2024). The dynamics generated by academic output alongside the production of societal know-how is vital to military capability development. Though these dynamics may result in diverging views and disrupt development processes (Leydesdorff, 2011), it may also have quite constructive effects. For instance, when knowledge transfer occurs between defence industry and the civilian domain, civilian companies tend to adapt their own research and development to better fit military needs (Sezal & Giumelli, 2022). This speaks to the potential of co-creation between government, industry and academia cooperating to identify various societal challenges as well as to optimise military capability development (Liwång, 2022). However, without effective interaction between policy processes on the one side and technology development on the other, capability development runs the risk of being curbed (Liwång, 2022). To illustrate this, defence capability planning has faced criticism for being overly rigid and disproportionately focused on high-cost investments, such

as fighter aircraft and air defence systems, while overlooking emerging technologies like AI and its potential to enhance interlinked capabilities (Liwång, 2022). Integrating emerging technologies with established defence capabilities therefore comes across as efforts riddled with obstacles (Wang et al., 2020). Also, adaptability during unexpected events or abrupt changes in customer needs, vary significantly at the production-level of industries (Wang et al., 2020). Since the outbreak of the war in Ukraine, these issues have become more apparent, revealing the complexity of policy-making for military capability development across Europe.

Involving a variety of organisations and institutions in collaborations is seen as a way to provide additional perspectives. It is argued that universities and research institutes together with industries and government institutions could elucidate important complexities that would otherwise go unnoticed and unresolved. This 'co-creation' would "[…] create an arena for trade-offs and debate […] creating a common understanding of the problems even if multiple values are present" (Liwång, 2022, p. 5). The idea of knowledge-sharing between academia, industry and government, also called the 'triple helix' model, is closely linked to the ideas of co-creation. While co-creation could be understood as the practical outcome, the ideas of a triple helix framework would correspond with its abstract or intellectual input. According to Klaus Bruno Schebesch et al., (2024), the potential of this intellectual networking lies to a great extent in creating long-term, transnational and polycentric cooperations to avoid the risk of capability development becoming trapped by fast-track success or hyped, deep-tech companies. Though their study is centred around smaller, commercial companies, quite far removed from governmentally controlled companies in the defence domain, it still offers useful insights. For instance, it suggests three factors that are universally important to ensure that any triple helix and co-creation process yields the desired output. First of all, a long-lasting acceptance by stakeholders (Schebesch et al., 2024). If applied to the context of military capability development, it is safe to say that the required acceptance is already in place at the national or supra-national levels in Europe. This is reflected in the numerous bilateral defence industrial projects (Calcara & Simón, 2024), and the European Defence Industrial Strategy (Clapp, 2024). Second, intellectual and entrepreneurial freedom (Schebesch et al., 2024), the very scaffolding for academia and entrepreneurship, is also evident when innovation allows to move beyond established technological trajectories (Bellais, 2023). The third factor for triple helix and co-creation frameworks to be successful is to ensure a strong foundation of common goals (Bellais, 2023). This would involve identifying and aligning shared objectives for military capability development across policymakers, industry, and academia. Given the differences between these three domains, this may prove to be particularly challenging - especially if stakeholders define and communicate the concept of capability development in divergent ways.

Diverging conceptualisations of 'capability development'

'Military capability development' may have quite different inferences for politicians, for military strategists, for the defence industry and for government organisations. In diplomatic and foreign relations, 'military capability' refers to the effectiveness of coercive, military power though when national budgets are being discussed, the concept is instead tied to relations with industrial suppliers (Giry & Smith, 2019). Taking Sweden as an example, the definition of military capability is influenced by the country's evolving role in EU's security and defence cooperation. However, though Swedish policymakers emphasise alignment with EU strategic defence initiatives (Swedish Ministry of Defence, 2024), Swedish defence industrial companies remain cautious due to the perceived, financial risks associated with EU initiatives (Håkansson, 2021). Such contrasting views illustrate how different domains – the executive, political level compared to stake-holders in the defence industry - assign different meanings, that may influence diverging priorities regarding military capability development. The findings by Giry and Smith (2019) suggest that even if stakeholders from different domains are cooperating towards a common goal, the concept may still be perceived quite differently, depending on domains. For example, collaboration between government, industry, and academia can be hindered by differing priorities and incentives. Among other things this creates a need for long-term strategies (de Spiegeleire, 2011; Liwång, 2022). This argument suggests that stake-holders' differing notions of 'military capability' may be detrimental to its development. Insufficient conceptual coherence is considered one of the impediments to British defence acquisition, leading to inefficiencies in planning and procurement (Yue & Henshaw, 2009). What is more, when abstract and value-laden concepts such as 'threat', 'risk', and 'innovation' – frequently used in capability planning - are added to the context - communication between actors and organisations is likely to become both knowingly and unknowingly simplified (Leydesdorff, 2011). This challenge is further discussed in terms of capabilities-based planning systems, where Thomas Young (2021) claims that "…what cannot be explained with precision cannot be understood with absolute clarity." (Young, 2021, p. 97). It is further argued that if 'capabilities' are defined only in relation to threat scenarios, they are unlikely to be effectively prioritised or planned for. This limited approach makes it difficult to integrate clear threats, political priorities (*as set out in policy*), and financial constraints when developing multi-functional capabilities like platforms (Young, 2021, p. 97).

A lack of conceptual coherence across sectors may lead to miscommunication, misconceptions, and missed opportunities, particularly when decisions have cross-sectoral implications for military capabilities. It is likely that achieving effective cooperation among the many interrelated branches and domains involved in military capability development requires a more holistic approach (Henshaw et al., 2011). In response to this need, the normative ecosystem model may provide a useful framework for guiding cross-sector collaboration. As

previously discussed, this model has the potential to capture the breadth and complexity of military capability development. However, it may also risk introducing additional conceptual ambiguity into an already intricate system. The following section explores both the advantages and the limitations of applying the ecosystem model in this context.

The Normative Ecosystem Model: A Conceptual Framework

An 'ecosystem' model describes and highlights interactions among highly complex elements (Tan & Chang, 2008). Its descriptive capacity is useful in itself, offering a way to capture what previous sections have exemplified and discussed. That is, the evolving nature of military capability development, along with its interdependencies. Due to such complexities, the model inherently involves elements of idealisation and simplification, reflecting a conceptual rather than literal representation of reality (Beck & Jahn, 2020). However, this paper also recognises the model's potential to provide actionable guidance to decision-makers and stakeholders, which means it would have a normative capacity that goes beyond its descriptive design (Beck & Jahn, 2020). Using a normative ecosystem model can help identify both internal and external influences, thereby enabling a more holistic understanding (Tan & Chang, 2008) of military capability development. By conceptualising the model as a network of interdependent relationships, processes, and cyclic interactions, it may serve as a tool for clarifying dynamic interplays and enhancing coordination among decision-makers and stakeholders. This, in turn, could encourage a shift from analysing capability entities in isolation to one that identifies interconnection and mutual influences. One example of this approach in practice is the European Commission Joint Research Centre's [JRC] use of the ecosystem model as an analytical framework to assess potential cascade effects from hybrid threats (European Commission, 2023). Drawing from several case studies, the JRC study concludes that, for effective foresight and decision-making, it is essential to recognise and understand the multi-layered interconnections within an ecosystem (European Commission, 2023). One of the model's key strengths is considered to be its ability to help uncover layered opportunities and constraints, thereby aiding decision-makers to navigate the intricacies of enhancing societal resilience against hybrid threats (European Commission, 2023). This suggests that such a model is capable of creating actionable output (Beck & Jahn, 2020).

However, all models inevitably involve elements of idealisation and simplification, serving as conceptual rather than literal representations of reality (Beck & Jahn, 2020). Thus, it is important to acknowledge that any normative ecosystem model faces the inherent challenge of translating complex, interconnected dynamics into concrete guidance - particularly in a domain as multifaceted as military capability development. Despite this, the normative ecosystem model appears useful for offering a broader systems-level understanding of military capability development, and to enable more integrated and adaptive

decision-making. Thus, it may encourage stakeholders to consider the required networking for private-public defence collaboration (de Spiegeleire, 2011) and could contribute to capability coordination and planning (Beck & Jahn, 2021).

Considering the Normative Ecosystem Model

As this paper has explicated earlier, defence and innovation initiatives have been closely linked for decades in several European countries. These initiatives are partly fuelled by the fear of being overshadowed by the United States in these matters (Martins & Mawdsley, 2021; Caverley, 2023). This particular narrative is claimed to equal that of a collectively held vision, spurring these countries to seek strategic autonomy and to influence their policymaking (Giry & Smith, 2019; Martins & Mawdsley, 2021; Bellais, 2023; Calcara & Simón, 2024). This policy-shaping characteristic is an important prerequisite shared by other normative models that have been successfully applied (Beck & Jahn, 2021). Therefore, such a model may prove both relevant and applicable, as military capability development is surrounded by policymaking in interconnected domains such as security, international relations and national industrial projects.

Considering the European Defence Industrial Strategy, which aims to enhance collaboration among member states (Ostanina & Tardy, 2024), the model could potentially promote policy alignment. However, the effectiveness of such alignment depends on the model's ability to capture not only possible, but in fact also improbable future scenarios along with the strength of incentives for stakeholders to act on its guidance (Beck & Jahn, 2021). Normative models are therefore suggested to play a catalytic role by identifying new areas for analysis and encouraging interdisciplinary research that integrates diverse knowledge and methods to drive defence-related innovation (Leydesdorff, 2011). Consequently, there is a strong relationship between historical practices, the influence of past strategic policy decisions, and the extent to which actions are either reinforced or constrained by institutionalised norms (Beck & Jahn, 2021). Acknowledging this may provide a way to identify and understand what is required to achieve a thriving and balanced ecosystem for military capability development. Furthermore, the model may serve to identify key elements both within itself, as well as interactions outside of it, along with their interdependencies.

However, to successfully implement a normative model, it is equally important to link abstract ideas to concrete components - both feasible as well as improbable ones (Knuuttila, 2017). This broadens the model's scope, allowing it to account for not only opportunities and weaknesses but also what may be considered irrelevant or unfeasible. The more effective an ecosystem model is of highlighting consequential factors beyond its immediate boundaries, the more relevant it becomes (Koskinen, 2022). The Future Combat Air System [FCAS] project - an ambitious collaboration between France, Germany, and to a lesser extent Spain -

illustrates this. France, with its strong defence industry, could opt out of such cooperation, while Germany benefits by leveraging its commercial strengths. These national differences are unlikely to change. While external to the ecosystem, they nonetheless affect its dynamics. Recognising such constraints as part of the model's relevance aligns with Tarja Knuuttila's (2017) and Rami Koskinen's (2022) emphasis on incorporating external contingencies to better understand the system's real-world implications.

As with any theoretical framework, the strengths of the normative ecosystem model need to be weighed against its shortcomings. One of its potential drawbacks is that it could lead discussions and decision-making into an overly complex web of interconnections, creating a network so vast it becomes impractical. If stretched too far, the concept of 'military capability development' risks becoming so broad that it loses conceptual clarity, undermining the potential for effective cross-sector collaboration. The question is whether international organisations, or decision-makers involved in multilateral industrial projects or even stakeholders at a national level have the capacity to treat military capability development with such a holistic approach. To take this criticism even further, all models are regarded as hypothetical systems – idealised versions of reality - which means they are never meant to be de-constructed, and are therefore highly abstract entities (Knuuttila, 2017). Hence, their value is often considered too vague and will rarely transcend from an intellectual activity to anything more concrete. As has been mentioned earlier, the risk is in part concerned with discussions moving too far into the theoretical and relying too much on analogies and metaphors (Knuuttila, 2017). There are also other, but similar, scholarly concerns about applying a holistic approach: Circling back to the discussion about the benefits of triple helix and cross-sectional co-creation, Loet Leydesdorff claims that "when more than two helices are involved, all bets are off, since various kinds of chaotic behaviour become possible" (2011, p. 28). Thus, it is fair to question whether additional, analytical perspectives generated by the ecosystem model would provide better guidance for practitioners and stakeholders alike. Still, as noted earlier regarding a model's descriptive capacity, the ecosystem as an analogy can in itself be valuable for facilitating communication. Indeed, this communicative function may represent one of the primary strengths of the model. In this way, its most fundamental role could be as a tool for building common understanding. Notwithstanding this, in order to expect concrete outcome of the ecosystem model, its intricacies need to be managed. One way to enhance its normative and actionable values is to apply it within a specific domain and at a particular point in time.

Yet, it is interesting that criticism towards a normative model that fails to promote achievable goals, may in fact spark innovative ideas (Leydesdorff, 2011). This silver-lining notion leads back to the discussion regarding inherent modality of normative models. In short, despite having immediately applicable outcomes, they still have the potential of inducing new ways to identify challenges and solutions. This, in turn, could create other, valuable

expectations besides delivering concrete solutions (Knuuttila, 2017). For example, the ecosystem model may serve as a productive analytical starting point by encouraging policymakers and military stakeholders to ask more targeted questions. One such question might be: which element within the capability development ecosystem is so critical that its removal would significantly disrupt the overall structure? Another inquiry could explore whether introducing a new policy or process would destabilise the system or, conversely, enhance its resilience.

Although the normative ecosystem model is an inherently abstract framework, representing an idealised, or at least simplified, perspective on capability development, it may prove effective for understanding complex and often intangible dynamics. In the very least, it could facilitate the translation of conceptual reasoning into practical guidance for real-world decision-making.

Conclusion

This discussion paper set out to investigate and consider patterns and tensions in European military capability development. It explored 'capability development' both as a theoretical concept and as an area of empirical research, highlighting the importance of knowledge transfer among academia, industry, and government. Additionally, it considered potential benefits and limitations of recognising capability development as an ecosystem, using this perspective to inform a normative model that helps identify interdependencies, improve coordination, and guide future capability planning. The main objective of this paper was to prompt further reflection on the utility of such a model for policy and practice. While the normative ecosystem model presents certain conceptual and practical challenges, the paper argues that applying such a model promotes a more integrated understanding of how military capabilities co-evolve. This paper argues that the model's primary values lie in enhancing the relevance of research and development, improving cross-domain communication, and in promoting a more nuanced debate. That said, conceptual clarity and clearly defined objectives are essential. A key question is therefore to ask what the is model intended to achieve - and for whom. The answer will determine whether its application is best pursued with cautious experimentation, strategic alignment, or both.

To build on the discussions in this paper, testing the model empirically would provide valuable insights. For instance, cyber warfare and artificial intelligence are driving defence innovation across several European countries and have the potential to generate new military capabilities. However, these rapidly emerging technologies may also result in unintended effects on national defence industries, that could affect operational readiness for more traditional defence domains (Ricart, 2023). Hence, applying the model to identify and analyse structural bottlenecks in today's defence supply chains for these technologies, such as policy

and decision-making, could provide actionable findings. What is more, examining and evaluating the model's applicability may help illustrate how technological development in one domain can reverberate across others, depending on shifting resources and strategic priorities. For instance, it could shed light on the opportunities and challenges of integrating new technologies into conventional capabilities at both the operational level and the tactical. Lastly, to apply the model for studying knowledge transfer between sectors and domains such as academia, emerging tech and established defence industries, as well as government institutions, would offer policy-relevant insights. Such research has the potential to deepen our understanding of how the ecosystem model can be used to strengthen military capability development across Europe.

References

Beck, L. & Jahn, M., (2021). Normative Models and Their Success, *Philosophy of the Social Sciences 2021, Vol. 51(2):* 123–150, https://doi.org/10.1177/0048393120970908

Bellais, R., (2023). Market Structures, Competition and Innovation: Grounds for an Alternative Defence Industrial Policy, *Defence and Peace Economics, 20 Feb:* 1-16, https://doi.org/10.1080/10242694.2023.2182869

Calcara, A. & Simón, L., (2024). Face to face: France, Germany and the future of the European defence industry, *Journal of European Public Policy:*1-25, https://doi.org/10.1080/13501763.2024.2358112

Caverley, J. D., (2023). Horses, nails, and messages: Three defense industries of the Ukraine war, *Contemporary Security Policy, 24 Sep:*1-18, https://doi.org/10.1080/13523260.2023.2257965

Chovančík, M., (2018). Defense industrialization in small countries: Policies in Czechia and Slovakia, *Comparative Strategy, 37:4*, 272-285, https://doi.org/10.1080/14751798.2025.2449771

Clapp, S., (2024). *European defence industrial strategy* [Briefing]. European Parliamentary Research Service. https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/762402/EPRS_BRI(2024)762402_EN.pdf

Ditrych, O. & Kucera, T., (2023). Defence cooperation and change: How defence industry integration fostered development of the European security community, *Cooperation and Conflict 2023, Vol. 58(1):* 129–152, https://doi.org/10.1177/00108367221099086

de Spiegeleire, S., (2011),Ten Trends in Capability Planning for Defence and Security, *The RUSI Journal, 156:5*, 20-28, https://doi.org/10.1080/03071847.2011.626270

European Commission, Joint Research Centre, & Centre of Excellence for Countering Hybrid Threats, (2023), *Hybrid threats – A comprehensive resilience ecosystem.* Science for Policy Report. Publications Office of the European Union. https://doi.org/10.2760/37899

Fabbrini, F., (2025). A Shield for Europe: Reviving the European Defence Community, *Survival, 67*:(1), 55-60. https://doi.org/10.1080/00396338.2025.2459016

Giry, B. & Smith, A., (2020). Defence capability in the UK since 2010: explaining change in procurement practices, *British Politics,15,* 433–455. https://doi.org/10.1057/s41293-019-00125-4

Henshaw, M., Kemp, D., Lister, P., Daw, A.J, Harding, A.D., Farncombe, A., Touchin, M., (2011). Capability Engineering – An Analysis of Perspectives, *INCOSE International Symposium, 2011-06, Vol.21 (1):* 712-727. https://doi-org.proxy.annalindhbiblioteket.se/10.1002/j.2334-5837.2011.tb01238.x

Håkansson, C., (2021). Finding its way in EU security and defence cooperation:

A view from Sweden, *European view, 2021-04, Vol.20* (1): 80-87. https://doi.org/10.1177/17816858211004647
Koskinen, R., (2023). Kinds of modalities and modeling practices, *Synthese 201*:(196), 1-16. https://doi.org/10.1007/s11229-023-04185-4
Knuuttila, T., (2017). Imagination extended and embedded: artifactual versus fictional accounts of models, *Synthese (Dordrecht), Vol.198* (S21)*:* S5077-S5097. https://doi.org/10.1007/s11229-017-1545-2
Krpec, O. & Kříž, Z., (2025). Structural challenges in adapting to
modern warfare: lessons from the Ukrainian War and the Czech defence industry, *Defense & Security Analysis, 41* (1), 1-28. https://doi.org/10.1080/14751798.2025.2449771
Leydesdorff, L., (2012). The Triple Helix, Quadruple Helix, …, and an N-Tuple of Helices: Explanatory Models for Analyzing the Knowledge-Based Economy?, *Journal of the knowledge economy, Vol.3* (1), 25-35. https://doi.org/10.1007/s13132-011-0049-4
Liwång, H., (2022). Defense development: The role of co-creation in filling the gap between policy-makers and technology development, *Technology in Society, 68:* 1-10. https://doi.org/10.1016/j.techsoc.2022.101913
Liwång, H., Liwång, Andersson, K., Bang, M., Malmio, I., & Tärnholm, T., (2023) How can systemic perspectives on defence capability development be strengthened?, *Defence Studies, 23*(3), 399-420, https://doi.org/10.1080/14702436.2023.2239722
Malmio, I., (2024). Can security be sustainable? Three perspectives on security and social sustainability: paradox, co-production, and deconstruction, *Sustainability Science, 19* (2), 615–627., https://doi.org/10.1007/s11625-023-01450-w
Martins, B. O. & Mawdsley, J. (2021). Sociotechnical Imaginaries of EU Defence: The Past and the Future in the European Defence Fund, *JCMS, Vol.59* (6), 1458-1474. https://doi.org/10.1111/jcms.13197
Mueller, T., (2025), Strategic options for the European defence industry in the 2020s, *Defense & Security Analysis, 41*(1), 49-80, https://doi.org/10.1080/14751798.2024.2418163
Olsen, G. R., (2022), Transatlantic cooperation in flux: Europe's small and cautious steps towards "strategic autonomy", *Defence Studies, 22*(4), 609-623. https://doi.org/10.1080/14702436.2022.2110477
Ostanina, S. & Tardy, T. (2024), Turbo-charging the EU's defence industry and security posture (Policy Brief), *Hertie School, Jacque Delors Centre,* 1-16. 20240417_EDIS_Paper_Ostanina_Tardy.pdf
Ricart, R. J. (2023). NATO defense innovation and deep tech: Measuring willingness and effectiveness. *Carnegie Endowment for International Peace*. https://carnegieendowment.org/
Schebesch, K. B., Soim, H. F. & Blaga, R. L. (2024). The triple-helix model as foundation of innovative entrepreneurial ecosystems, *Journal of Ethics in Entrepreneurship and Technology, Vol.4*(2), 104-129. http://dx.doi.org/10.1108/JEET-08-2024-0026
Sezal, M. A. & Giumelli, F. (2022). Technology transfer and defence sector dynamics: the case of the Netherlands, *European Security, 31*(4), 558-575. https://doi.org/10.1002/smj.3137
Siebold, S. & Bayer, L. (2025), Pentagon chief confident NATO will commit to Trump's defence spending target, *Reuters*, *https://www.reuters.com/business/aerospace-defense/nato-ministers-discuss-defence-spending-hike-ahead-key-summit-2025-06-05* [June 13, 2025]
Swedish Government, (2023). *Statement of government policy, 12 September 2023.* Regeringskansliet [Government Offices of Sweden]. https://www.government.se/speeches/2023/09/statement-of-government-policy-12-september-2023
Swedish Ministry of Defence, (2024). *Strategisk inriktning för försvarsinnovation* [Strategic direction for defence innovation]. Regeringskansliet [Government Offices of Sweden].

https://www.regeringen.se/contentassets/38380ae279be406a9775a6d54002503e/strategisk-inriktning-for-forsvarsinnovation.pdf

Tan, A. & Chang, V., (2008), An Ecosystem Approach to Knowledge Management: Case Studies of Two Australian SMEs, *19th Australasian Conference on Information Systems,* 967-979.

Wang, T., Aggarwal, V.A., Wu, B., (2020). Capability interactions and adaptation to demand-side change, *Strategic Management Journal, 41,* 1595-1627. https://doi.org/10.1080/09662839.2022.2028277

Yue, Y. & Henshaw, M., (2009), An Holistic View of UK Military Capability Development, *Defense & Security Analysis, 25*(1), 53-67, https://doi.org/10.1080/14751790902749900

Young, T. (2021). Capabilities-Based “Confusion”: Why Capabilities-Based Planning Systems Struggle, *The Korean Journal of Defense Analysis Vol. 33, No. 1:* 95-118, https://doi.org/10.22883/kjda.2021.33.1.005

Chapter 22: Enhancing European Ammunition Production: Strategic Responses and Challenges

Ass. Prof. Roland **Hellberg**, https://orcid.org/0000-0001-8972-7975
Ass. Prof. Martin **Lundmark**, https://orcid.org/0000-0002-1197-8173

Abstract:
The high ammunition consumption by Ukrainian armed forces has created unprecedented demand, surpassing Europe's peace-optimized supply capacity by far. To address this, the EU and individual states are offering financial support to manufacturers, including initiatives like the Act in Support of Ammunition Production [ASAP]. However, such financial stimuli pose challenges in countries like Sweden, where state ownership influence is absent, and procurement follows strict public regulations. Beyond investment hesitancy, manufacturers face raw material shortages and limited access to critical components like primers, gunpowder, and explosives. Scaling production requires expanding supplier capacity, securing skilled labour, and obtaining permits and land for new facilities. This study examines how to build a resilient ammunition supply chain and manage state-industry relations when governments intervene financially. Empirical data were collected from official documents, public service news, and industry interviews in Sweden. Findings emphasize the need for robustness, resilience, and flexibility to respond to security threats. Nations must rebuild strategic, trust-based ties with defence firms, reversing the effects of the New Public Management [NPM] transformation. To adapt, manufacturers and states must enhance dynamic capabilities and develop stable yet innovative solutions and strengthen Europe's strategic autonomy in defence. These insights will aid policymakers, procurement authorities, defence forces, and manufacturers in sustaining and expanding ammunition production.

Keywords: ammunition manufacturing, supply chain, dynamic capability, strategic autonomy

Introduction

The impact of the Ukraine conflict on defence production and supply

The ongoing conflict in Ukraine has sharply increased demand for defence materiel, surpassing existing production and supply capacities (EU Commission, 2024a; Boot, 2024). Donor nations have supplied Ukraine with equipment and ammunition while also boosting domestic orders to replenish stockpiles (Freyrie, 2023). In response, the European Union [EU] plans to expand ammunition production, targeting 1.3 million shells in 2024 (SvD, 2024; EU Commission, 2024c; Fabbrini, 2024; Mueller, 2024). However, limited coordination and inadequate manufacturing capacity hinder military support efforts (DN, 2024a; McNeil, 2024a).

Individual nations have adopted varied procurement strategies, increasing defence budgets to enhance military capabilities (Fiott, 2024; IISS, 2025). As a result, defence manufacturers face surging orders, but pre-existing production capacities, designed for a stable and peace-optimized security environment, are insufficient, causing backlogs. While firms strive to maximize output, they remain dependent on suppliers for critical components. Expanding production also requires stronger commitment from the state, priority, more rapid decision processes and skilled personnel and regulatory approvals (Hellberg & Lundmark, 2025).

State involvement in the defence industry varies in form. Sweden procures from independent suppliers, while Finland and Norway maintain partial state ownership of domestic defence firms, enabling greater strategic influence (Brzoska, 2006; Hagelin, 2006; Lundmark, 2022). Regardless of ownership, production capacity is constrained by manufacturing limitations and supplier reliability.

EU support measures depend on the capabilities of individual member states. Governments aim to strengthen supply chain resilience but must balance control, influence, and market regulations. EU legislation allows states to designate specific defence products as national essential security interests, enabling direct procurement while bypassing restrictions on subsidies and market distortions (EU Directive, 2009/81).

Previous research

Existing research highlights key challenges and opportunities in the European ammunition industry amid shifting geopolitical dynamics. Lee and Mittal (2022) identify steel shortages as a major bottleneck, while Piotrowski (2023) stresses the need for manufacturers to adapt to rising demand. Sebastian (2023) and Studies (2023) emphasize the European Peace Facility's role in strengthening regional defence by facilitating procurement. Initiatives like the European Chips Act and the Critical Raw Materials Act aim to improve supply chain resilience and production capacity.

Santamaria et al. (2023) point to shortages of metal casings for medium-calibre rounds, leading to cost overruns and production delays. Aries et al. (2023) note that low historical demand has reduced industrial capacity, making manufacturers hesitant to invest without long-term commitments. The surge in defence budgets post-Ukraine invasion has driven procurement, often favouring non-EU suppliers.

Fabbrini (2024) sees the Act in Support of Ammunition Production [ASAP] as a step toward an integrated European defence union, aligning military capabilities with industrial needs. ASAP is unique in that it was the first time that subsidies for supporting defence firms' production capacity was directly financed through the EU budget. Supply chain vulnerabilities persist, with Hellberg and Lundmark (2025) noting a shift from transactional to trust-based

contracts to enhance resilience. Zhelikhovskyi (2024) examines EU efforts to boost Ukraine's ammunition production through foreign investment and aid.

Despite extensive research, the impact of public subsidies on corporate behaviour and ammunition production remains unexplored. Further study is needed to assess how government support influences industry expansion and long-term scalability

Research objectives

This research aims to analyse the evolving dynamics of interactions among defence firms, national governments, and supranational agencies in the context of increasing ammunition production to meet sharply rising demand. Specifically, it explores how a resilient ammunition supply chain can be established and examines the challenges inherent in state intervention through financial stimulus in the defence industry. The study is guided by the following key research questions:

RQ1: What factors impede the production capacity of ammunition manufacturers?

RQ2: How can national governments and the EU act to establish long-term resilience in the ammunition supply chain, and what risks are associated with such interventions?

RQ3: What contractual and regulatory considerations must be addressed in the relationship between the state and private defence firms to ensure a sustainable and credible long-term framework when financial stimuli are provided?

These questions will be analysed within a broader context of ammunition supply chains and will be more closely grounded in the Swedish context and conditions. Sweden serves as an interesting example due to earlier far-reaching defence acquisition reforms in peace-time and that there is no state ownership in the defence industry. Following the introduction, the paper is structured as follows. The next section outlines the research methods employed in this study, followed by the theoretical framework, which draws on the concepts of *Strategic autonomy*, *Supply chain dependencies* and *Dynamic Capabilities*. The subsequent section presents the research findings and discusses their implications. Finally, the paper concludes with a summary of key insights and suggestions for future research.

Methodology

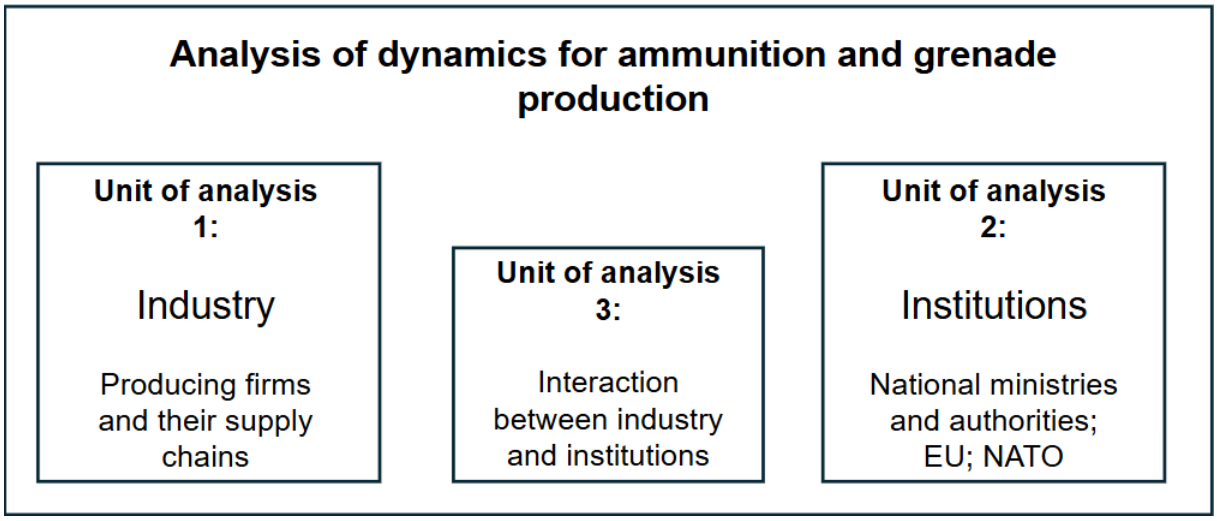
The empirical data for this study has been obtained from a diverse range of sources, including official documents, published analyses, public service news, and interviews. Targeted searches were conducted on official documents from EU authorities and the Swedish government, focusing on the study's core themes.

Several individual interviews were conducted during 2024/25 with representatives from the ammunition industry in Swedish firms and the Swedish Defence Materiel Administration Agency (FMV). Each interview, lasting approximately 90 minutes, was conducted in person

and recorded. The interviews followed a semi-structured format, incorporating open-ended questions to facilitate in-depth discussions and capture nuanced perspectives. For confidentiality reasons, all interviews have been anonymized, and no direct quotations are included in this study. This research incorporates three key units of analysis:

- Defence firms operating in Sweden, examining their roles, strategies, and constraints.
- Institutions, analysing their influence, with a focus on the EU, the Swedish state, and associate authorities.
- Inter-institutional and corporate relationships, assessing interactions and interdependencies between institutional and corporate actors.

Figure 22.1:*Units of Analysis*



A qualitative approach was employed for data analysis, utilizing a modified version of targeted thematic content analysis. Thematic analysis is used to identify common patterns within the data, enhancing the understanding of various statements and observations (Morgan, 1993; Braun & Clarke, 2006; Mayring, 2023). In targeted content analysis, the initial coding process is informed by pre-existing theories or prior research (Hsieh & Shannon, 2005; Funck & Karlsson, 2021). The directed content analysis applied in this study seeks to explain relationships across the three levels of analysis while identifying dependencies and risks within the defence production and supply framework. The theoretical framework guided the coding process, ensuring consistency and analytical depth.

Theoretical framework

As Europe's security situation deteriorates, states increasingly demand continuous replenishment of defence supplies (Fabbrini, 2024). The concept of security of supply ensures

the availability of critical defence resources (Moran & Russell, 2008; Fjäder, 2014; van Kampen et al., 2016; Besch, 2016; Sani et al., 2022; Department of Defense Report, 2022a). While maintaining inventory or using substitutes has traditionally been costlier than demand-based procurement (Fisher, 1997; Pagh & Cooper, 1998; Lee, 2002; Christopher et al., 2006; Basnet & Seuring, 2016), worsening security conditions have shifted EU policy toward greater *strategic autonomy*, reducing reliance on non-EU suppliers (EU Commission, 2020; SWD, 2021). The EU's Strategic Compass strengthens European security while addressing supply chain vulnerabilities (EU Union, 2022; Helwig, 2021; Kleczka et al., 2024).

The surge in demand for ammunition and grenades has intensified the focus on how states ensure access to the munitions they require. Concepts such as *strategic autonomy, sovereign capability, security of supply*, and *autarky* are increasingly employed by both individual states and the European Union to address this issue in similar ways.

"*Sovereign capability*" refers to a nation's self-sufficiency in defence, public health, and essential resources (Black et al., 2021; Worrall et al., 2021; MoD, 2024). "*Strategic autonomy*" has become a focal concept in the EU defence discourse. In this context, it concerns how Europe can attain increased self-reliance in arms development and production and to decrease Europe's dependency on foreign technology – especially vis-à-vis the US (Kleczka et al, 2024; Borrell, 2024). However, full security of supply is unattainable due to globalized manufacturing and resource dependencies (Lieb-Dóczy et al., 2003; Zsidisin & Ellram, 2003; Teer & Bertolini, 2022). Instead, strategic stockpiling and diversified procurement are necessary (Chiaramonti & Maniatis, 2020). Ensuring security of supply requires risk assessment, strategic partnerships, redundancy in suppliers, and international collaboration (Svensson, 2000; Jüttner et al., 2003; Walter et al., 2003; Stevenson & Spring, 2007; Tangpong et al., 2015; Stewart & Ivanov, 2022). International collaboration, interoperability, and the use of substitutes are essential components of this strategy (Stevenson & Spring, 2007; Moran & Russell, 2008; Hall et al., 2010; Fjäder, 2014; Fevolden & Tvetbråten, 2016; van Kampen et al., 2016; Pernin, 2019; Sani et al., 2022). Partnerships with allied nations to ensure mutual support, supply chain mapping to identify critical nodes, maintaining buffer stocks of essential materials and domestic production capacity are critical (Lind & Press, 2018; Fonseca & Azevedo, 2020; Vinod Kumar & Gurbani, 2022).

Production flexibility can be achieved through outsourcing, shift work, and expanded production lines (Sheffi, 2005; Tang, 2006; Tomlin, 2006; Tørhaug, 2006). A robust supply chain design mitigates vulnerabilities and disruptions (Park, 2011; Purvis et al., 2016; Park et al., 2016; Simchi-Levi et al., 2018). A robust strategy emphasizes an organization's ability to anticipate and respond to unforeseen risks, recover quickly from disruptions, and resume normal or improved operations (Park, 2011; Cohen & Kouvelis, 2021; Gutierrez et al., 2022). The COVID-19 pandemic revealed vulnerabilities in supply chains, especially in defence

manufacturing, which heavily relies on global suppliers (Department of Defence [Australia], 2020; 2022 Antai & Hellberg, 2023). For instance, ammunition manufacturing supply chains are predominantly global due to the lack of raw materials and component manufacturing capabilities in many nations (Hochschorner et al., 2006; Markowski et al., 2009; Dimitrov & Hall, 2013; Santamaria et al., 2023). The current security climate underscores the risks associated with reliance on suppliers outside national borders (Europaportalen, 2022), prompting both the EU and individual states to seek greater sovereign capabilities.

From 1990 to 2010, New Public Management (NPM) influenced defence procurement, emphasizing competition, privatization, and cost efficiency (Hood, 1995; Grimsey & Lewis, 2004; Guay, 2007; Ettinger, 2011). The UK led in privatizing government-owned defence assets and outsourcing non-core government services, while France, Italy, and Spain pursued partial privatization. Many European firms still retain state influence over the defence industry (Markowski & Wylie, 2007). Sweden, by contrast, adopted a market-liberal model, relying on private-sector defence firms, allowing defence firms to operate without state ownership (Lundberg & Rova, 2022; Lundmark, 2022). Without state ownership, it is not possible to direct or influence a company during peacetime. Globalized procurement has fragmented supply chains, increasing vulnerabilities amid geopolitical tensions (Kolk & van Tulder, 2010; Bode & Wagner, 2015).

Strategic partnerships between governments and defence suppliers that mitigate risks has become increasingly common (Ministry of Defence, 2021). Maintaining a domestic defence industry ensures adaptability, justifying investment despite costs (DeVore, 2021). As firms pursue globalization for cost advantages, they also face greater disruption risks (Stevenson & Spring, 2007; Mackay et al., 2020). Conflicts and wars highlight the need for defence supply chain resilience (Durach et al., 2015; Monostori, 2018). Political uncertainty has driven firms to reshore production and relocate to stable regions (Blackhurst et al., 2011; Lundmark, 2014; Stentoft et al., 2015; Hartman et al., 2017; Loska & Higa, 2020; Gao et al., 2022; Department of Defense Report, 2022b).

The Ukraine war has underscored the need for the defence industry to scale up defence production during crises (Kovács & Tatham, 2009; Schoeni et al., 2023). Sweden, lacking state ownership in defence firms, relies on public procurement under market conditions, except in areas classified as essential security interests (Hellberg, 2023). EU Directive 2009/81 allows exemptions for national security procurement (Bratanova, 2004; Gombos & Szűcs, 2019). EU states apply these rules differently, with some categorizing more defence equipment as security-critical (Weiss & Blauberger, 2016; Meershoek, 2021; Gov. UK, 2021). In Sweden, defence firms do not maintain excess production capacity unless contractually obligated (Hellberg, 2023).

The EU supports defence modernization through coordinated capability development within both the EU and NATO (Major & Mölling, 2019). The Act in Support of Ammunition Production, adopted in July 2023, enhances EU ammunition production without distorting markets (EU Commission, 2024c; Fabbrini, 2024). This initiative enables states to provide targeted support to the defence industry without it being considered a market-distorting subsidy.

Understanding the networks and the institutional context for defence procurement is crucial for management of defence supply chains. These networks involve complex interdependencies between suppliers, buyers, users, regulators, and government actors up to the ministerial level (Chavi et al., 2022; Fletcher-Chen et al., 2022; Hellberg & Lundmark, 2025). The current market situation places significant pressure on defence firms. Even if they wish to expand production, they cannot act independently. Arms trade, ammunition production, and defence materiel procurement are subject to numerous laws and regulations that all involved parties must comply with (Sigma, 2011). Defence firms cannot expand production independently, as they rely on suppliers for raw materials, components, as well as machinery and spare parts providers (Ford et al., 2011; Kurc & Oktay, 2018; Aries et al., 2023; Kleczka et al., 2024; Bardt, 2024).

The industrial network approach highlights trust and interdependence in business relationships (Axelrod, 1984; Johanson & Mattsson, 1987; Axelsson & Easton, 1992; Carr & Pearson, 1999; Walter, 2003; Håkansson & Gadde, 2018; Gadde, 2021). Scholars argue that organizations must develop "*dynamic capabilities*": to possess a capability to adapt to and capitalize on unexpected market changes and environmental transformations (Teece et al., 1997; Eisenhardt & Martin, 2000; Teece, 2010; Yoho et al., 2013). To sum up the theoretical framework: We aim to analyse the corporate sector; the national and supranational institutional sector; and the interaction between the two.

Findings

Global demand for ammunition and grenades surged significantly in 2022 due to three interrelated factors. First, countries sought to replenish depleted stockpiles after donating substantial quantities of munitions to Ukraine. Second, many states increased their war reserve levels as part of broader, long-term rearmament strategies. Third, there was a sustained and urgent commitment to provide Ukraine with the ammunition necessary to support its ongoing defence efforts. As a result, demand within Europe approximately tripled (Hellberg & Lundmark, 2025).

At the start of 2022, EU countries produced approximately 230,000 155mm artillery shells annually, about one-third more than the U.S. By February 2023, production increased to 300,000 rounds per year, reaching 400,000 by November (Skove, 2023). Following

measures implemented in 2023, the EU's annual production capacity hit one million shells by January 2024 (EU Commission, 2024a).

Despite urgent procurement efforts, global production capacity remains far below demand. Years of geopolitical stability led ammunition manufacturers to streamline production for moderate demand. The production capacity overall became optimized for a stable security situation in a peace-time context. Many Western producers have extensive international order backlogs, causing long delivery times. Additionally, supply chains optimized for cost-efficiency and just-in-time operations are not designed for handling sudden demand surges. The closure of industrial facilities and consolidation of chemical and explosive suppliers into a few firms further constrains production (Ruitenberg, 2024). Notably, only 20–25% of EU-supplied weapons are produced within the EU-bloc, with the rest sourced externally (The Kyiv Independent, 2024).

The European Commission allocated €513 million from the combined budgets of the EU and Norway under the ASAP initiative, enabling the European defence industry to increase its ammunition production capacity to 2 million shells annually by the end of 2025 (EU Commission, 2024a; Department of Defense, 2025). The primary objective of the ASAP initiative is to meet Ukraine's operational needs (ENDR, 2023; EU Defence Industry, 2023).

The Commission completed the evaluation under the ASAP and selected 31 projects to assist European industry in increasing its ammunition production and readiness. The selected projects cover five areas: explosives, powder, shells, missiles, and testing and reconditioning certification. Attachment 1 illustrates U.S. and EU efforts to expand ammunition manufacturing, highlighting the long lead times required to build up production capacity (Department of Defense, 2025). The EU Commission formulated the principles of ASAP as follows:

> The selected projects cover five areas: explosives, powder, shells, missiles, and testing and reconditioning certification. The projects will be funded with €513 million from the budgets of the EU and Norway. This funding will leverage additional investment from industry through co-financing, resulting in a total investment of around €1.4 billion in the supply chain. ASAP focuses on powder and explosives, which are bottlenecks for ammunition shell production, and will allocate some three quarters of the programme to them. The programme will support projects increasing the annual production capacity by more than 10 000 tonnes of powder, and by more than 4 300 tonnes of explosives. For this purpose, The Union will invest €248 million in powder manufacturing capacity and €124 million in explosives manufacturing capacity (EU Commission 2024a).

This funding covers between 35% and 45% of project costs, with EU contributions ranging from €2 million to €65 million per initiative. The remaining 55% to 65% must be secured by participating firms through alternative financing sources (Försvarsdepartementet, 2022; EU Defence Industry, 2023). Member states may further support these efforts through procurement or direct financial assistance. Eligibility for funding is primarily based on a project's potential to expand production capacity and reduce lead times (Försvarsdepartementet, 2022; EU Defence Industry, 2023; Teknik och Säkerhetsforum, 2023).

However, this expansion depends on sustained and long-term government orders, which remain insufficient. Without long-term contracts, Europe is unlikely to sustainably scale ammunition production for Ukraine in the coming years (The Kyiv Independent, 2024). A report by European Security & Defence (2025) details expansion efforts by Nordic defence manufacturer Nammo, which is increasing production of 155mm shells, 120mm tank rounds, and AIM-120 AMRAAM rocket motors under a 15-year, EUR 86 million contract signed with Norway in July 2024. Nammo's Swedish factory, funded by the EU's ASAP initiative and the Swedish government, is set to triple 155mm ammunition production, while its Finnish operations expand 155mm shells, nitrocellulose, and explosives.

Despite these efforts, securing raw materials and components remains a challenge. Lower-tier suppliers in the defence supply chain face mounting pressure to meet rising demand. As European Security & Defence (2025) warns, "Organizations face an existential threat due to supply chain visibility issues, impacting operational efficiency, financial stability, ethical compliance, national security, and environmental sustainability."

Expanding ammunition production capacity extends beyond merely increasing personnel, machinery, and physical space; distinct bottlenecks exist not only within the production process itself but also throughout the upstream supply chain. For instance, shell casings are manufactured in Norway and Finland, while one of the essential explosives is produced in Poland, necessitating coordinated efforts across multiple countries (DN, 2024b).

To reduce dependence on bottleneck suppliers, the Nammo Group has announced its plan to construct a new primer factory in Finland. This facility, representing an investment of EUR 33 million, is scheduled to become operational in 2025 and reach full capacity by 2027 (SK, 2024).

The availability of TNT in Europe is critically low. The only factory within the EU is in Poland; however, its production capacity is insufficient to meet the high demand. Consequently, initiatives have been launched in both Finland and Sweden to reduce reliance on TNT imports and establish domestic production. A planned Swedish facility is expected to produce TNT for 450,000 shells per year, with similar plans underway in Finland (Yle, 2024; NyTeknik, 2025; SvT, 2025).

In addition to these supply chain challenges, ammunition manufacturers face further constraints in expanding production capacity. The primary obstacles include securing long-term financial coverage for investments and obtaining the necessary permits for increased production and storage of explosives.

Perspective of ammunition producers operating in Sweden

Within the framework of Nordic Defence Cooperation [Nordefco], Nammo has been awarded a contract worth approximately NOK 600 million for the supply of artillery ammunition to Ukraine. Norway, Sweden, and Denmark are each contributing roughly one-third of the funding. These contracts further support the firm's increased production capacity (Stortinget, 2023). Nordic defence cooperation began in 2009, primarily aiming to enhance each country's defence capabilities and strengthen their ability to act together in the event of a regional crisis (Regeringskansliet, 2023).

In the current context of a significant surge in ammunition demand, manufacturers are in a favourable negotiating position. However, somewhat paradoxically from an external perspective, firms are reluctant to rely on financing from a single customer, as this could lead to dependency and lock-in effects. In the specific case of Sweden, the major ammunition manufacturer is owned by the Norwegian and Finnish governments, which introduces potential conflicts of interest regarding the financing of a Swedish customer. Consequently, the structure of financing contracts is of critical importance, not only for ensuring long-term cost coverage and production volume but also for maintaining the operational autonomy of firms. This is ultimately a matter of *strategic autonomy* and long-term risk distribution among various stakeholders.

Beyond state subsidies, securing favourable investment financing for ammunition production remains challenging due to prevailing financial market policies and regulations. Most financial institutions have explicit policies against funding weapons manufacturing, further restricting access to capital.

Acquiring production equipment for ammunition manufacturing presents additional difficulties due to limited supply. High product quality standards necessitate that certain production processes be developed in-house, which prolongs the procurement process for new equipment. Furthermore, establishing new production facilities requires extensive measures to ensure protection and security against external threats, adding further complexity to the expansion process.

A high production volume presupposes minimal adjustments in production resources. However, in the current situation, customers have varying specification requirements, necessitating frequent modifications to production lines. The ammunition produced is certified by the customer for specific artillery systems. Another constraint arises from the unique

material and component specifications imposed by different customers. This means that manufacturers cannot mix deliveries from different suppliers without explicit customer approval. Such approvals take considerable time to obtain, as they require extensive testing and validation. This inhibits standardization between nations and within the EU.

Two critical considerations emerge when states provide support to enhance ammunition manufacturing capabilities: first, the specific requirements and technical specifications of their own defence forces, and second, the distinct specifications of the ammunition needed by Ukraine or other international recipients.

Swedish institutional perspective

The war in Ukraine and the surge in global demand have driven many nations to strengthen coordination with domestic suppliers. This shift marks a transition from a market-driven, competitive procurement model to long-term, trust-based partnerships. These agreements align firms' strategic objectives with financial realities, enhancing national war readiness.

Since March 2018[1] and August 2022[2], Sweden, Finland, and Norway have coordinated strategies to achieve greater self-sufficiency in ammunition production, including critical components such as ignition caps. This collaboration extends beyond these nations, as they seek to act collectively as a larger customer to increase their leverage in the ammunition market. While involved stakeholders recognize the need to standardize ammunition specifications within the Nordic region, significant resistance persists due to variations in artillery systems, differing approval processes for ammunition, and specific labelling requirements.

As previously mentioned, a key challenge in Sweden's ammunition procurement is that Nammo is jointly owned by the Norwegian and Finnish governments. In 2024, the FMV partnered with Nammo to support the ASAP initiative, which aims to expand artillery ammunition production. This investment, co-financed by the Swedish government and the European Union, received EU funding in early 2024 (FMV, 2024).

Expanding industrial capacity and strengthening domestic production requires further investments and agreements (Försvarsdepartementet, 2024a). To facilitate targeted procurement processes and co-financing the expansion of production capacity, the Swedish government has designated security of supply of ammunition as an essential security interest.

[1] In 2018, an intergovernmental agreement was concluded between the governments of Denmark, Finland, Norway, and Sweden regarding cooperation in the field of defence materiel. A specific section of this agreement, referred to as the "Annex," addresses the security of supply for ammunition.
[2] In 2022, "Arrangement E" was implemented by the governments of Denmark, Finland, Norway, and Sweden as a supplement to the Annex concerning Security of Supply for Ammunition, which forms part of their intergovernmental agreement on cooperation in the field of ammunition.

The FMV recognize the need to navigate the legal framework effectively and secure the ability to enter long-term contracts.

From a Swedish perspective, discussions have taken place regarding which firms should receive investment. Strategic location is also a crucial consideration, as suppliers must be capable of delivering even in times of crisis and war. Additionally, potential state ownership stakes in ammunition manufacturers have been considered, but in the absence of a comprehensive Swedish defence industry strategy, government agencies remain uncertain about the preferred course of action. When the state acts as an investor, questions arise concerning ownership and control of the investment, specifically, what should be produced and for whom?

Inter-institutional and corporate relationships

One of the key obstacles to *strategic autonomy* is securing sufficient funding for expanded production. Private financial institutions often restrict investments in defence manufacturing due to ethical and policy considerations, making state-backed funding and EU financial support crucial. Initiatives such as the ASAP program, which Sweden is jointly pursuing with the EU, are essential for sustaining production growth. However, competition for EU funding and the complexities of multinational financing create additional challenges.

Beyond financial concerns, logistical constraints also limit the ability to rapidly scale production. Expanding industrial capacity requires access to specialized machinery, skilled labour, and regulatory approvals for increased production and storage of explosives. These processes take time, adding to the difficulty of achieving full strategic independence in the short term.

How different companies finance these projects remains unclear, but there are indications that customers place long-term orders with a certain surcharge to cover investment costs. Naturally, companies must arrange financing or leasing for production equipment themselves, but the sources of these funds are not publicly disclosed. It is likely a mix of the companies' own capital, state guarantees, and financial institutions willing to provide loans to the arms industry. For example, Rheinmetall received over €130 million under ASAP, reflecting public-private collaboration to reinforce Europe's defence sector. Its expansion extends beyond Germany to Estonia, Hungary, Romania, and Spain (McNeil, 2024b). The EU expects ASAP to enable the production of two million artillery shells annually by late 2025 (EU Commission, 2024b).

In March 2024, Sweden and Nammo secured EU support to expand ammunition production (SvT, 2024; Försvarsdepartementet, 2024b). Similarly, Norwegian firms Nammo Raufoss, Kongsberg Defence and Aerospace, and Chemring Nobel received EU funding, alongside 950 million NOK in state support (VG, 2024).

Grenade production requires increased powder and explosive output. The Commission emphasized that powder and explosives are critical bottlenecks, and the programme will support projects increasing the annual production capacity by more than 10 000 tonnes of powder (for 1.3 million shells) and, and by more than 4 300 tonnes of explosives (for 800,000 shells). For this purpose, The Union will invest €248 million in powder manufacturing capacity and €124 million in explosives manufacturing capacity (EU Commission, 2024a; Politico, 2024).

ASAP aligns with the EU's *strategic autonomy* goals, a priority accelerated by the Ukraine war (Verellen & Hofer, 2023). Hoffmeister (2023) notes that this pursuit has led to new EU trade policy tools, with ASAP reinforcing this trajectory.

Despite these investments, production capacity remains insufficient to meet rising demand. Expanding facilities alone is not enough, specialized skills and raw materials are also essential. Currently, supplier numbers remain limited, and most production facilities rely on the same key suppliers. According to industry experts, it will take 1–2 years before these investments yield the intended production output. A deeper understanding of supply chain interdependencies is crucial to enhancing European ammunition production capabilities.

Conclusion

Russia's expansionist ambitions culminated in the full-scale invasion of Ukraine in 2022. In response, EU nations prioritized both the supply of ammunition to Ukraine and the strengthening of their own national defence capabilities. However, this revealed significant challenges in rapidly scaling the production capacity of ammunition and grenade supply chains. Achieving such an upscaling required substantial investment, which firms were initially reluctant to undertake without external support. As a result, both national governments and the EU introduced financial mechanisms to stimulate production. The overall preparedness of the pre-2022 supply chains proved insufficient, and the necessary *dynamic capabilities* to respond to the altered security landscape were lacking.

Existing supply chains faced notable bottlenecks, particularly in the supply of chemicals, explosives, and essential components. The EU's ASAP initiative helped address these shortfalls by financing cross-border supplier networks. In Sweden's case, the partnership with Nammo, despite its Norwegian and Finnish ownership, demonstrated how regional collaboration and state-backed support can transform such firms into strategic production hubs. A stable and credible long-term demand for ammunition and grenades, coupled with strong political will, is likely to incentivize firms to invest in capacity expansion, thereby sharing in both the risks and the financing.

Robust supply chains cannot be created or maintained by states alone. Firms and their associated networks constitute the operational backbone of defence supply, and as such,

must be supported, nurtured, and developed. These supply chains must not only become more robust, resilient, and flexible, but must also meet the aggregate demand generated by three concurrent needs: the continuous supply to Ukraine's armed forces, the replenishment of donated munitions, and the buildup of national war reserves across Europe.

Given the cross-border dependencies within these supply chains, national and EU-wide agreements have become essential. Strengthened supply chains are now seen as critical to developing the EU's sovereign defence capabilities in the face of ongoing security threats. This has required a deepening of the strategic interface between states and firms. The shift from a peacetime, contract-based market model to a more trust-based, long-term strategic partnership between government and industry is now underway.

To facilitate this shift, states must support business models that are viable for firms, ensuring their willingness to expand production. This has involved forms of state investment that were previously restricted under EU competition laws. Sweden, for example, has designated the security of ammunition supply as a essential national security interest, thus enabling targeted, non-competitive procurement.

Sweden operates within a broader institutional framework defined by EU regulations, NATO obligations, and cross-border industrial dependencies. The balance between EU and NATO has become increasingly uncertain, particularly considering recent political developments in the United States. This instability has further motivated the European Commission to strengthen its coordination of EU defence procurement and capability development, efforts aimed at enhancing the EU's *strategic autonomy* and reducing dependence on U.S. support.

By fostering reliable, robust, and resilient supply chains through trust-based partnerships with industry, Sweden and the European Union aim to develop credible *dynamic capabilities*. These, in turn, are essential to building sovereign defence capacities that can endure and adapt to present and future security challenges. To summarize the first RQ: *What factors impede the production capacity of ammunition manufacturers?* Several key factors influence Sweden's ammunition production capacity, as:

1. *Supply chain dependencies:* Ammunition manufacturers rely on imported components such as ignition caps and explosives, requiring international coordination and creating supply vulnerabilities.
2. *Quality standards & specialized production:* High-quality requirements limit rapid scaling, as specialized machinery and production processes often need to be developed in-house.
3. *Undeveloped state-industry relationships:* Centred on existing short-term contracts rather than on long-term, trust-based strategic agreements.

4. *Regulatory frameworks:* Lengthy permit processes for increasing production and storing explosives create administrative hurdles that slow down expansion efforts.
5. *Financial constraints:* Private financial institutions are hesitant to fund arms manufacturing, necessitating reliance on state-backed investments and EU funding.
6. *Ownership structures & strategic autonomy:* Sweden's dependence on Nammo, a firm co-owned by Norway and Finland, raises concerns about national control over ammunition supply and decision-making.

To summarize the second RQ: *How can national governments and the EU act to establish long-term resilience in the ammunition supply chain, and what risks are associated with such interventions?* To enhance long-term resilience in the ammunition supply chain, national governments and the EU can take the following measures:

1. *State-backed investments & EU funding:* Given private sector reluctance to finance arms production, direct government investments and EU-backed programs (such as the ASAP initiative) are essential for securing sustainable funding.
2. *Long-term procurement agreements:* Shifting from market-driven procurement to stable, trust-based contracts can provide manufacturers with financial security and encourage investment in production expansion.
3. *Regional cooperation:* Sweden, Finland, and Norway have taken steps to enhance regional self-sufficiency; however, further standardization of artillery systems, ammunition types, and procurement processes is necessary to improve interoperability and efficiency.

The interventions under consideration carry several risks. Heavy government involvement may create market distortions that reduce competition, generate inefficiencies, and ultimately raise costs. Increased state oversight can also introduce regulatory and bureaucratic delays, slowing efforts to expand production capacity. In addition, Sweden's dependence on Nammo—a company co-owned by Norway and Finland—raises the possibility of conflicting national interests during periods of crisis. Finally, a strong reliance on EU and NATO initiatives risks making Sweden vulnerable to shifts in international policy and funding priorities, potentially constraining its ability to act independently when strategic conditions change.

To summarize the third RQ: *What contractual and regulatory considerations must be addressed in the relationship between the state and private defence firms to ensure a sustainable and credible long-term framework when financial stimuli is provided?* For a

sustainable and credible long-term framework, the following contractual and regulatory considerations must be addressed:

1. *Stable, long-term contracts:* Governments should establish multi-year procurement agreements with private manufacturers to ensure financial stability and incentivize investments in production capacity. However, there must be a balance in contract models to avoid locking the state into arrangements that hinder competition, limit innovation, or result in overreliance on suppliers that fail to adapt or improve.
2. *Clear investment guidelines:* A well-defined Swedish defence industry strategy is needed to clarify the state's role in ownership, funding, and regulatory oversight of ammunition production.
3. *Balanced regulation:* While safety and security regulations are essential, excessive bureaucracy can hinder production expansion. Regulatory processes should be streamlined without compromising oversight.
4. *Risk-sharing mechanisms:* The government should consider shared financial responsibility models, where private firms receive conditional funding based on meeting production and delivery targets.

Final thoughts and future research

This research makes a theoretical contribution by expanding the concept of *security of supply* to incorporate strategic partnerships, industrial policy, and subsidy-driven capacity-building. It extends prior studies on security of supply by demonstrating how geopolitical instability and rising defence expenditures are shifting procurement strategies from demand-driven models (Fisher, 1997; Pagh & Cooper, 1998) toward long-term *strategic autonomy* (EU Commission, 2020; SWD, 2021).

Building on existing conceptualizations of *sovereign capability* (Black et al., 2021; Worrall et al., 2021) and *strategic autonomy* (Kleczka et al, 2024; Borrell, 2024), this study highlights the practical challenges of achieving self-sufficiency in munition production amid globalized manufacturing dependencies (Lieb-Dóczy et al., 2003; Zsidisin & Ellram, 2003). These findings underscore the critical role of *dynamic capabilities* in defence manufacturing (Teece et al., 1997; Eisenhardt & Martin, 2000; Teece, 2010), as firms must navigate unpredictable demand surges while ensuring operational stability. The analysis further reveals that Sweden and other EU countries are increasingly recognizing the vulnerabilities of a purely market-driven procurement approach, particularly in times of crisis, thereby reinforcing calls for *state intervention and long-term investment strategies* (DeVore, 2021; Lundmark, 2022).

While previous research has examined state influence in the defence industry (Markowski & Wylie, 2007), this study *explicitly links EU funding mechanisms such as the*

ASAP, to long-term industrial capacity-building and the pursuit of *strategic autonomy*. It offers empirical insights into how EU member states are navigating the balance between NATO commitments and regional defence industrial policies, supporting arguments that *defence procurement is becoming increasingly regionalized in response to growing geopolitical instability* (Verellen & Hofer, 2023). The study also highlights the potential risks associated with this approach, including reduced competition, supply chain vulnerabilities, and overdependence on regional actors.

The insights from this research will benefit political decision-makers, procurement authorities, defence forces, and ammunition manufacturers by providing a deeper understanding of the conditions necessary for ammunition manufacturing. While this study provides valuable insights into munition production capacity, supply chain resilience, and state-industry relations, further research is needed in the following areas:

- Exploration of different state-industry partnership models, including hybrid ownership structures, to ensure long-term supply security.
- An assessment of the risks and benefits of Sweden taking an ownership stake in domestic ammunition manufacturers.
- Strategies for Sweden to reduce reliance on imported components by developing domestic production capacity for key materials such as explosives and ignition caps.
- The impact of Sweden's NATO membership on its ammunition procurement and production strategies.

Addressing these research gaps will contribute to a more comprehensive understanding of how Sweden and Europe can enhance defence production capacity, *strategic autonomy*, and industrial sustainability.

References

Antai, I., & Hellberg, R. (2023). Identifying total defense logistics concepts: a comparative study of the Swedish pandemic response. *Journal of Humanitarian Logistics and Supply Chain Management*, 14(2), 208-222.

Aries, H., Giegerich, B., & Lawrenson, T. (2023). The GUNS of Europe: Defence-industrial challenges in a time of war. *Survival*: June-July (pp.7-23), Routledge.

Axelrod, R. (1984). *The evolution of cooperation*. Basic Books, New York.

Axelsson, B., & Easton, G. (eds.) (1992). *Industrial Networks: A New View of Reality*. Routledge: London.

Bardt, H. (2024). Industrial Policy and a Single Market for Defence Goods. *Intereconomics*, 6.

Basnet, C., & Seuring, S. (2016). Demand-oriented Supply Chain Strategies – A Review of Literature. *Operations and Supply Chain Management*, 9(2).

Besch, S. (2016). *Security of supply in EU defence: Friends in need?* CER insight. Centre for European Reform, London.

Black, J., Flint, R., Harris, R., Galai, K., Paillé, P., Quimbre, F., & Plumridge, J. (2021). *Understanding the Value of Defence: Towards a Defence Value Proposition for the UK.* RAND Corporation, Santa Monica, CA.
Blackhurst, J., Dunn, K.S., & Craighead, C.W. (2011). An Empirically Derived Framework of Global Supply Resiliency. *Journal of Business Logistics*, 32, 374-391.
Bode, C., & Wagner, S.M. (2015). Structural drivers of upstream supply chain complexity and the frequency of supply chain disruptions. *Journal of Operations Management,* 36, 215-228.
Boot, M. (2024). *Weapons of War: The Race between Russia and Ukraine.* Council on Foreign Relations. https://www.cfr.org/expert-brief/weapons-war-race-between-russia-and-ukraine
Borrell, J. (2024, March 11). Time to strengthen European defence industry. *The Diplomatic Service of the European Union*. https://www.eeas.europa.eu
Bratanova, E. (2004). *Legal Limits of the National Defence Privilege in the European Union*. Paper 34, Bonn International Center for Conversion, Germany.
Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative research in psychology, 3(2), 77-101.
Brzoska, M. (2006). The Nordic attitude to and role in EU-linked defence industrial collaboration. In Bailes, A. J., Herolf, G., & Sundelius, B. (Eds.). (2006). *The Nordic countries and the European security and defence policy*. Oxford University Press.
Carr, A.S., & Pearson, J.N. (1999). Strategically managed buyer–supplier relationships and performance outcomes. *Journal of Operations Management*, 17, 497-519.
Chavi, C.Y., Sharma, A., & Rangarajan, D. (2022). Examining supplier, buyer, and customer triads: The critical role of conflict in interaction processes and product/service innovations. *Industrial Marketing Management*, 107, 337-352.
Chiaramonti, D., & Maniatis, K. (2020). Security of supply, strategic storage and Covid19: Which lessons learnt for renewable and recycled carbon fuels, and their future role in decarbonizing transport? *Applied Energy*, 271.
Christopher, M., Peck, H., & Towill, D. (2006). A taxonomy for selecting global supply chain strategies. *The International Journal of Logistics Management*, 17(2).
Cohen, M.A., & Kouvelis, P. (2021). Revisit of AAA excellence of global value chains: Robustness, resilience, and realignment. *Production and Operations Management*, 30(3).
Department of Defence (Australia) (2020). *Defence Strategic Update 2020*. https://www.defence.gov.au/about/publications/2020-defence-strategic-update
Department of Defence (Australia) (2022). *Securing Australia's Defence Supply Chains*. AI Group, Defence Council. https://www.aigroup.com.au/globalassets/news/reports/2022/defence-supply-chain-report-280822.pdf
Department of Defense (2025). *Fact Sheet on Efforts of Ukraine Defense Contact Group National Armaments Directors*, Jan. 10. https://www.defense.gov/News/Releases/Release/Article/4026238/fact-sheet-on-efforts-of-ukraine-defense-contact-group-national-armaments-direc/
Department of Defense Report (2022a). *State of Competition within the Defense Industrial Base*. Office of the Under Secretary of Defense for Acquisition and Sustainment, US.
Department of Defense Report, (2022b). *Securing Defense-Critical Supply Chains -An action plan developed in response to President Biden's Executive Order 14017*. https://media.defense.gov/2022/Feb/24/2002944158/-1/-1/1/DOD-EO-14017-REPORT-SECURING-DEFENSE-CRITICAL-SUPPLY-CHAINS.PDF
DeVore, M.R. (2021). Armaments after autonomy: Military adaptation and the drive for domestic defence industries. *Journal of Strategic Studies*, 44(3), 325-359.
Dimitrov, D., & Hall, P. (2013). Small arms and light weapons production as part of a national and global defence industry. *Small Arms, Crime and Conflict*, 207-227.
DN (2024a). *Skyller ifrån sig om sena vapenleveranser*. Artikel 2024-01-30. https://www.dn.se/varlden/skyller-ifran-sig-om-sena-vapenleveranser/

DN (2024b). *Här försöker de jaga ikapp det ryska övertaget*. Artikel 2024-02-12. https://www.dn.se/sverige/har-forsoker-de-jaga-ikapp-det-ryska-overtaget/

Durach, C.F., Wieland, A., & Machuca, J.A.D. (2015). Antecedents and dimensions of supply chain robustness: a systematic literature review. *International Journal of Physical Distribution & Logistics Management,* 45(1/2), 118-137.

Eisenhardt, K.M., & Martin, J.A. (2000). Dynamic capabilities: what are they? *Strategic management journal,* 21(10-11), 1105-1121.

ENDR European network of defence-related regions (2023). *Act in Support of Ammunition Production*. https://endr.eu/news/2023-05-03-258/act-in-support-of-ammunition-production/

Ettinger, A. (2011). Neoliberalism and the rise of the private military industry. *International Journal*, 66(3), 743-764.

EU Commission (2020). *EU Directive on defence and sensitive security procurement*. https://defence-industry-space.ec.europa.eu/eu-defence-industry/defence-procurement_en

EU Commission (2024a). *The Commission allocates €500 million to ramp up ammunition production, out of a total of €2 billion to strengthen EU's defence industry*. https://defence-industry-space.ec.europa.eu/around-eu2-billion-strengthen-eus-defence-industry-readiness-including-ramp-ammunition-production-2-2024-03-15_en

EU Commission (2024b). *The Commission allocates €500 million to ramp up ammunition production, out of a total of €2 billion to strengthen EU's defence industry*. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1495

EU Commission (2024c). *ASAP Results Factsheet 15 MARCH 2024*. https://defence-industry-space.ec.europa.eu/regulation-support-ammunition-production-asap-aims-reinforcing-and-ramping-ammunition-production_en

EU Defence Industry (2023). *The Act in Support of Ammunition Production (ASAP) at a glance*. https://defence-industry-space.ec.europa.eu/eu-defence-industry/asap-boosting-defence-production_en

EU Directive 2009/81. *EC on the award of contracts in the fields of defence and security*. Guidance Note Offsets.

EU Union (2022). *A Strategic Compass for Security and Defence: For a European Union that protects its citizens, values and interests and contributes to international peace and security*. https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf

Europaportalen (2022). *EU countries are concerned about American protectionism*. https://www-europaportalen-se.translate.goog/2022/10/eu-lander-oroas-av-amerikansk-protektionism?_x_tr_sl=sv&_x_tr_tl=en&_x_tr_hl=sv&_x_tr_pto=wapp

European Security & Defence (ESD) (2025). *Just in time is dead: How European manufacturers are gearing up for land warfare.* https://euro-sd.com/2025/01/articles/42257/just-in-time-is-dead-how-european-manufacturers-are-gearing-up-for-land-warfare/

Fabbrini, F. (2024). European Defence Union ASAP: The Act in Support of Ammunition Production and the development of EU defence capabilities in response to the war in Ukraine. *European Foreign Affairs Review*, 29(1), 67- 84.

Fevolden, A.M., & Tvetbråten, K. (2016). Defence industrial policy – a sound security strategy or an economic fallacy? *Defence Studies*, 16 (2), 176–192.

Fiott, D. (2024). From liberalisation to industrial policy: Towards a geoeconomic turn in the European defence market? *Journal of Common Market Studies*, 62, 1012–1027.

Fisher, M.L. (1997). What is the right supply chain for your product? *Harvard Business Review,* 75(2).

Fjäder, C. (2014). The nation-state, national security and resilience in the age of globalisation. *Resilience*, 2(2).

Fletcher-Chen, C.C.Y., Sharma, A., & Rangarajan, D. (2022). Examining supplier, buyer, and customer triads: The critical role of conflict in interaction processes and product/service innovations. *Industrial marketing management*, 107, 337-352.
FMV (2024). *Avtal om ökad produktion av artilleriammunition*. https://www.fmv.se/aktuellt--press/aktuella-handelser/avtal-om-okad-produktion-av-artilleriammunition/
Fonseca, L.M., & Azevedo, A.L. (2020). COVID-19: outcomes for global supply chains. *Management & Marketing. Challenges for the Knowledge Society*, 15.
Ford, D., Gadde, L.E., Hakansson, H., & Snehota, I. (2011) *Managing business relationships*. John Wiley & Sons.
Försvarsdepartementet (2022). *Förordning om stöd för ammunitionsproduktion (ASAP).* 2022/23:FPM94.
Försvarsdepartementet (2024a). *Stärkt försvarsförmåga - Sverige som allierad*. Ds 2024:6.
Försvarsdepartementet (2024b). *EU financial support for increased ammunition production in Sweden.* https://www.government.se/press-releases/2024/03/eu-financial-support-for-increased-ammunition-production-in-sweden/
Freyrie, M. (2023). Industrial production in support of European and transatlantic defence. *Istituto Affari Internazionali* (IAI).
Funck, E.K., & Karlsson, T.S. (2021). *Handbok för systematiska litteratur- och dokumentstudier inom samhällsvetenskapen*. Förvaltningshögskolans rapporter nummer 158.
Gadde, L.E. (2021). From channel management towards network coordination – changing perspectives on distribution arrangements. *Journal of Business & Industrial Marketing*, 36(13), 42-53.
Gao, X., Hewings, G.J.D., & Yang, C. (2022). Offshore, re-shore, re-offshore: what happened to global manufacturing location between 2007 and 2014? *Cambridge Journal of Regions, Economy and Society*, 15(2), 183-206.
Gombos, K., & Szűcs, A.E. (2019). Review of the European union's regulation regarding defence procurement. *Economics and Management*, 28-34.
Gov. UK (2021). *Transforming Public Procurement - Government response to consultation*. https://www.gov.uk/government/consultations/green-paper-transforming-public-procurement/outcome/transforming-public-procurement-government-response-to-consultation#key-themes
Grimsey, D., & Lewis, M.K. (2004). *Public Private Partnerships – The Worldwide Revolution in Infrastructure Provision and Project Finance*. Edward Elgar Publishing Limited, Cheltenham, UK.
Guay, T.R. (2007). *Globalization and Its Implications for the Defense Industrial Base*. Monographs, Books, and Publications, 696, US Army War College.
Gutierrez, L., Lameijer, B.A., Aand, G., Antony, J., & Sunder M.V. (2022). Beyond efficiency: the role of lean practices and cultures in developing dynamic capabilities. *International Journal of Operations & Production Management*, 42(13).
Hagelin, B. (2006). Hardware politics, 'hard politics' or 'where, politics?': Nordic defence equipment cooperation in the EU context. In Bailes, A. J., Herolf, G., & Sundelius, B. (Eds.). (2006). *The Nordic countries and the European security and defence policy*. Oxford University Press.
Håkansson, H., & Gadde, L.E. (2018). Four decades of IMP research - the development of a research network. *IMP Journal*, 12(1), 6-36.
Hall, P., Markowski, S., & Wylie, R. (2010). *Supply.* In: (Eds) Markowski, Hall, Wylie, Defence Procurement and Industry Policy: A Small Country Perspective, Routledge.
Hartman, P.L., Ogden, J.A., Wirthlin, J.R., & Hazen, B.T. (2017). Nearshoring, reshoring, and insourcing: Moving beyond the total cost of ownership conversation. *Business Horizons*, 60(3), 363-373.
Hellberg, R. (2023). Swedish public procurement and the defence industry: obstacles and opportunities. *Journal of Defense Analytics and Logistics*, *7*(2), 103-137.

Hellberg, R., & Lundmark, M. (2025). Transformation in European Defence Supply Chains as Ukraine Conflict Fuels Demand. *Scandinavian Journal of Military Studies*, 8(1), 17–39.
Helwig, N. (Eds) (2021). *Strategic autonomy and the transformation of the EU: New agendas for security, diplomacy, trade and technology*. FIIA Report 67.
Hochschorner, E., Hägvall, J., Finnveden, G., Griffing, E., & Overcash, M. (2006). Environmental life cycle assessment of a pre-fragmented high explosive grenade. *Journal of Chemical Technology and Biotechnology*, 81(3), 461-475.
Hoffmeister, F. (2023). Strategic autonomy in the European Union's External Relations Law. *Common Market Law Review*, 60(3).
Hood, C. (1995). The "New Public Management" in the 1980s: Variations on a theme, *Accounting. Organizations and Society*, 20(2/3), 93-109.
Hsieh, H.F., & Shannon, S. (2005). Three Approaches to Qualitative Content Analysis. *Qualitative Health Research*, 15(9).
IISS (2025). *Global defence spending soars to new high*. https://www.iiss.org/online-analysis/military-balance/2025/02/global-defence-spending-soars-to-new-high/
Johanson, J., & Mattsson, L.G. (1987). Interorganizational relations in industrial systems – a network approach compared with the transaction-cost approach. *International Studies of Management and Organization*, 17(1), 34-48.
Jüttner, U., Peck, H., & Christopher, M. (2003). Supply Chain Risk Management: Outlining an Agenda for Future Research. *International Journal of Logistics: Research and Applications*, 6(5).
Kleczka, M., Vandercruysse, L., Buts, C., & Du Bois, C. (2024). The Spectrum of Strategic autonomy in EU Defence Supply Chains. *Defence and Peace Economics,* 35(4), 427-447.
Kolk, A., & van Tulder, R. (2010). International business, corporate social responsibility, and sustainable development. *International Business Review*, 19(2), 119-125.
Kovács, G., & Tatham, P. (2009). Responding to Disruptions in the Supply Network – From Dormant to Action. *Journal of Business Logistics*, 30(2), 215-229.
Kurc, C., & Oktay, S. (2018). Taking production relations seriously: the role of defence firms in armaments cooperation. *European Security*, 27(4), 469-489.
Lee, D., & Mittal, V. (2022). Identifying Potential Supply Chain Bottlenecks Within the Ammunition Manufacturing Process for the Optionally Manned Fighting Vehicle. *Industrial and Systems Engineering Review*, 10(2), 151-158.
Lee, H.L. (2002). Aligning Supply Chain Strategies with Product Uncertainties. *California Management Review,* 44(3).
Lieb-Dóczy, E., Börner, A-R., & MacKerron, G. (2003). Who Secures the Security of Supply? European Perspectives on Security, Competition, and Liability. *The Electricity Journal*, 16(10).
Lind, J., & Press, D.G. (2018). Markets or mercantilism? How China secures its energy supplies. *International Security*, 42(4).
Loska, D., & Higa, J. (2020). The risk to reconstitution: supply chain risk management for the future of the US Air Force's organic supply chain. *Journal of Defense Analytics and Logistics*, 4(1), 19-40.
Lundberg, A., & Rova, E. (2022). Management Reforms in the Defence Sector. *Defence and Peace Economics*, 33(4), 454-474.
Lundmark, M. (2014). Kockums - the Repatriation of the Swedish Underwater Crown Jewel. *Défense & Industries,* 1(7–8).
Lundmark, M. (2022). The Evolution Towards the Partial Strategic Autonomy of Sweden's Essential Security Interests. *Defence and Peace Economics*, 33(4), 399-420.
Mackay, J., Munoz, A., & Pepper, M. (2020). Conceptualising redundancy and flexibility towards supply chain robustness and resilience. *Journal of Risk Research*, 23(12), 1541-1561.
Major, C., & Mölling, C. (2019). PeSCo: The German Perspective. *ARES Group Policy Paper*, 36.

Markowski, S., & Wylie, R. (2007). The Emergence of European Defence and Defence Industry Policies. *Security Challenges*, 3(2), 31-51.
Markowski, S., Koorey, S., Hall, P., & Brauer, J. (2009). Multi-channel supply chain for illicit small arms. *Defence and Peace Economics*, 20(3), 171-191.
Mayring, P.A.E. (2023). *Qualitative content analysis*. In (eds) Tierney, R. J., Rizvi, F., & Ercikan, K. International Encyclopedia of Education (Fourth Edition). Elsevier.
McNeil, H. (2024a). GlobalData: supply chains pressured amidst global rearmament race. *Army Technology*, March 22.
McNeil, H. (2024b). EU boosts Rheinmetall with €130m to ramp up artillery production in Europe. *Army Technology*, April 2.
Meershoek, N. (2021). The Constraints of Power Structures on EU Integration and Regulation of Military Procurement. *European Papers*, 6(1), 831-868.
Ministry of Defence (2021). *Defence and Security Industrial Strategy: A strategic approach to the UK's defence and security industrial sectors*. CP 410, England.
MoD (2024). *Guidance DSPCR Chapter 13: security of supply*. https://www.gov.uk/government/publications/the-european-union-defence-and-security-public-contracts-regulations-dspcr-2011
Monostori, J. (2018). Supply chains robustness: Challenges and opportunities. *Procedia CIRP,* 67, 110-115.
Moran, D., & Russell, J.A. (Eds.) (2008). *Energy security and global politics: The militarization of resource management*, 6. Routledge.
Morgan, D.L. (1993). Qualitative content analysis: a guide to paths not taken. *Qualitative health research*, 3(1).
Mueller, T. (2024). Drivers and Impact of European Defence Market Integration: A Literature Meta-Synthesis with Economic Focus. *Defence and Peace Economics*, 1(36).
NyTeknik (2025). *Planen: Svensk fabrik för TNT – kan räcka till 450 000 granater per år.* https://www.nyteknik.se/industri/planen-svensk-fabrik-for-tnt-kan-racka-till-450-000-granater-per-ar/4326308
Pagh, J.D., & Cooper, M.C. (1998). Supply Chain Postponement and Speculation Strategies: How to choose the right Strategy? *Journal of Business Logistics*, 19(2).
Park, K. (2011). *Flexible and Redundant Supply Chain Practices to Build Strategic Supply Chain Resilience: Contingent and Resource-based Perspectives*. Doctor of Philosophy Degree in Manufacturing and Technology Management. The University of Toledo.
Park, K., Min, H., & Min, S. (2016). Inter-relationship among risk taking propensity, supply chain security practices, and supply chain disruption occurrence. *Journal of Purchasing and Supply Management*, 22(2).
Pernin, C.G., Hlávka, J.P., Boyer, M.E., Gordon, J.IV, Lerario, M., Osburg, J., Shurkin, M., & Gibson, D.C. (2019). *Targeted interoperability: A new imperative for multinational operations*. RAND.
Piotrowski, M.A. (2023). *EU Plans for Increased Ammunition Production*. PISM Polski Instytut Spraw Międzynarodowych.
Politico (2024). *EU doles out €500M for artillery ammunition and missiles as it seeks to match Russia*. https://www.politico.eu/article/eu-doles-out-e500m-for-artillery-ammo-and-missiles-as-it-seeks-to-match-russia/
Purvis, L., Spall, S., Naim, M., & Spiegler, V. (2016). Developing a resilient supply chain strategy during 'boom' and 'bust'. *Production planning & control*, 27(7-8).
Regeringskansliet (2023). *Det nordiska försvarssamarbetet Nordefco.*
Ruitenberg, R. (2024). France to spend $540 million on artillery propellant production. *Defense News*. https://www.defensenews.com/global/europe/2024/04/11/france-to-spend-540-million-on-artillery-propellant-production/
Sani, S., Schaefer, D., & Milisavljevic-Syed, J. (2022). Strategies for Achieving Pre-emptive Resilience in Military Supply Chains. *Procedia CIRP*, 107.
Santamaria, L.C.P., Yoo, M.S., & Mittal, V. (2023). The Impact of Supply Chain Issues on Military Training and Readiness, *Military Review*, 85-94.

Schoeni, D., Butler, L., & Trybus, M. (2023). *A Special Issue on The Emerging Impact of the Russian Invasion of Ukraine on Defence Procurement in Europe*, SSRN. https://ssrn.com/abstract=4636560

Sebastian, C. (2023). *Reinforcing the European defence industry*. EPRS: European Parliamentary Research Service. Belgium. https://coilink.org/20.500.12592/knm53z

Sheffi, Y. (2005). *The resilient enterprise: overcoming vulnerability for competitive advantage.* Pearson Education India.

Sigma (2011). *Brief 23 Defence Procurement*. Support for Improvement in Governance and Management.

Simchi-Levi, D., Wang, H., & Wei, Y. (2018). Increasing supply chain robustness through process flexibility and inventory. *Production and Operations Management*, 27(8), 1476-1491.

SK (2024). *Nammo builds primer factory in Vihtavuori, Finland.* https://sk-ammunition.com/nammo-builds-primer-factory-in-vihtavuori-finland/

Skove, S. (2023). In race to make artillery shells, US, EU see different results. *Defense One Today*. https://www.defenseone.com/business/2023/11/race-make-artillery-shells-us-eu-see-different-results/392288/

Stentoft, J., Mikkelsen, O.S., & Johnsen, T.E. (2015). Going Local: A Trend towards Insourcing of Production? *Supply Chain Forum: An International Journal,* 16(1), 2-13.

Stevenson, M., & Spring, M. (2007). Flexibility from a supply chain perspective: definition and review. *International Journal of Operations & Production Management*, 27(7), 685-713.

Stewart, M., & Ivanov, D. (2022). Design redundancy in agile and resilient humanitarian supply chains. *Annals of Operations Research*, 319(1).

Stortinget (2023). *Skriftlig spørsmål fra Ine Eriksen Søreide (H) til forsvarsministeren.* https://www.stortinget.no/no/Saker-og-publikasjoner/Sporsmal/Skriftlige-sporsmal-og-svar/Skriftlig-sporsmal/?qnid=87357

Studies, Ł. (2023). *OSW Commentary - ASAP: EU support for ammunition production in member states - Artillery ammunition: European needs and shortages*. Centre for Eastern Studies, Poland. https://coilink.org/20.500.12592/qqk79f

SvD (2024). *EU ökar granatproduktionen*. Artikel 2024-01-20.

Svensson, G. (2000). A Conceptual Framework for the Analysis of Vulnerability in Supply Chains. *International Journal of Physical Distribution & Logistics Management*, 30(9).

SvT (2024). *Svensk ammunitionsfabrik beviljas EU stöd*. https://www.svt.se/nyheter/inrikes/svensk-ammunitionsfabrik-beviljas-eu-stod-ska-tredubbla-produktionen

SvT (2025). *Företag planerar TNT-fabrik i Nora – tillverkar sprängämnen*. https://www.svt.se/nyheter/lokalt/orebro/planer-pa-tnt-fabrik-i-nora

SWD (2021). *Strategic dependencies and capacities, Commission Staff Working Document*. SWD/2021/352 final.

Tang, C.S. (2006). Robust Strategies for Mitigating Supply Chain Disruptions. *International Journal of Logistics: Research and Applications*, 9(1).

Tangpong, C., Michalisin, M.D., Traub, R.D., & Melcher, A.J. (2015). A review of buyer-supplier relationship typologies: progress, problems, and future directions. *Journal of Business & Industrial Marketing*, 30(2).

Teece, D. (2010). Business Models, Strategy and Innovation. *Long Range Planning,* 43(2-3), 172-194.

Teece, D.J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. *Strategic management journal*, 18(7), 509-533.

Teer, J., & Bertolini, M. (2022). *Survey outcome. Threats to the supply of critical raw materials for semiconductors.* The Hague Centre for Strategic Studies.

Teknik och Säkerhetsforum (2023). *Kamp om EU-pengar till ammunition*. Artikel 2023-12-13. https://www.tekniksakerhetsforum.se/artiklar/kamp-om-eu-pengar-till-ammunition

The Kyiv Independent (2024). *EU to produce 2 million artillery shells in 2025, new defense commissioner tells media*. Dec. 24. https://kyivindependent.com/eu-to-produce-2-million-artillery-shells-in-2025-new-defense-commissioner-tells-media/
Tomlin, B. (2006). On the Value of Mitigation and Contingency Strategies for Managing Supply Chain Disruption Risks. *Management Science*, 52(5).
Tørhaug, M. (2006). Petroleum Supply Vulnerability due to Terrorism at North Sea Oil and Gas Infrastructures. *In Protection of Civilian Infrastructure from Acts of Terrorism,* edit. Frolov, K.V., & Baecher, G.B. Springer.
van Kampen, T., van Fenema, P.C., & Faber, N. (2016). Strategic Defence Supply Chain Security Management. In: Beeres, R., Bakx, G., de Waard, E., Rietjens, S. (eds), NL ARMS Netherlands. *Annual Review of Military Studies 2016*. NL ARMS. T.M.C. Asser Press, The Hague.
Verellen, T., & Hofer, A. (2023). The Unilateral Turn in EU Trade and Investment Policy. *European Foreign Affairs Review*, 28(Special).
VG (2024). *Norsk forsvarsindustri får EU-penger til å produsere ammunisjon*. https://www.vg.no/nyheter/innenriks/i/WR9RMG/opplysninger-til-vg-norsk-forsvarsindustri-faar-eu-penger-til-ammunisjon
Vinod Kumar, S.V., & Gurbani, N.K. (2022). Managing Logistics and Supplies. In: Gupta, S.D. (eds) *Healthcare System Management.* Springer, Singapore.
Walter, A. (2003). Relationship-specific factors influencing supplier involvement in customer new product development. *Journal of Business Research*, 56, 721-733.
Walter, A., Müller, T.A., Helfert, G., & Ritter, T. (2003). Functions of industrial supplier relationships and their impact on relationship quality. *Industrial marketing management*, 32(2).
Weiss, M., & Blauberger, M. (2016). Judicialized Law-Making and Opportunistic Enforcement: Explaining the EU's Challenge of National Defence Offsets. *Journal of Common Market Studies,* 54, 444-462.
Worrall, L., Gamble, H., Spoehr, J., & Hordacre, A.L. (2021). *Australian sovereign capability and supply chain resilience: perspectives and options.* Australian Industrial Transformation Institute, College of Business, Government and Law. Flinders University of South Australia.
Yle (2024). *Försvarsminister Häkkänen bekräftar: Finland vill att det snabbt byggs en TNT-fabrik*. https://yle.fi/a/7-10056236
Yoho, K.D., Rietjens, S., & Tatham, P. (2013). Defence logistics: an important research field in need of researchers. *International Journal of Physical Distribution & Logistics Management*, 43(2), 80-96.
Zhelikhovskyi, S. (2024). *War and Industry*. International Centre for Defence and Security (ICDS).
Zsidisin, G.A., & Ellram, L. (2003). An agency theory investigation of supply risk management. *Journal of Supply Chain Management*, 39(3).

Attachment 1

US Department of Defense Jan. 10, 2025

Excerpt from: Fact Sheet on Efforts of Ukraine Defense Contact Group National Armaments Directors (Department of Defense, 2025)

Significant ammunition production achievements to date:

- **Expansion of existing, or establishment of new, production capacity of critical munitions around the world.**
  The United States has invested $5.5 billion to expand domestic production capacity of the following munitions or subcomponents *(NOTE: entries reflect increases from 2022 to current production rates)*:
  - 155mm Projectiles: 14,400 per month to 40,000 per month *(178% increase)*
  - 155mm Propelling Charge:14,494 per month to 18,000 per month *(24% increase)*
- **Examples of production expansion and munitions delivery efforts announced by UDCG members include, but are not limited to:**
  - Through the Act in Support of Ammunition Production (ASAP), European defense industry is expected to increase annual ammunition shell production capacity to 2 million by the end of 2025. 31 projects cover five areas: explosives, powder, shells, missiles, and testing and reconditioning certification.
  - France and Sweden will double capacity of ammunition and explosives loading by 2025, double capacity of modular charges by 2026, and increase powder production capacity ten-fold by 2026.
  - Sites in Germany, Spain, Hungary, South Africa, and Australia plan to increase production up to 700,000 artillery shells and up to 10,000 tons of gunpowder per year by 2025; this includes a new gunpowder factory in Romania as part of a project developed with the European Commission and a new artillery ammunition facility in Germany.
  - A consortium of 15 countries led by the Czech Republic have pledged €1.7 billion to source 500,000 artillery rounds from around the world by the end of 2024.
  - Norway will invest more than NOK 1 billion to significantly expand artillery production for at least 15 years.
  - Nordic other participating nations are increasing ammunition production through the NORDEFCO++ initiative to support Ukraine as well as to strengthen long-term capacity to ensure regional security of supply.
- **From 2023 to 2024, Ukraine increased its total domestic production of mortar and artillery ammunition, ranging from 60mm to 155mm calibers, from 1 million rounds to 2.5 million rounds annually** (150% increase).
  - Identification of gaps and mitigations for production of propellants and explosives.
  - Facilitation of, and support to, partnerships with Ukrainian industry for co-production and co-sustainment activities.
- **Examples of U.S.-Ukraine industry partnerships include:**
  - Northrop Grumman signed an agreement with the Government of Ukraine to provide equipment and training to establish a medium-caliber ammunition production line *(July 2024)*.
  - D&M Holding Company constructed an ammunition factory in Ukraine and are currently expanding production pursuant to agreements with the Ukrainian Ministry of Strategic Industries and key companies (October 2023).

- **Examples of international-Ukraine industry partnerships include:**
  - Nammo (Norway) announced that it will license production of 155mm rounds in Ukraine *(August 2024)*.
  - KNDS (France/Germany) is establishing a subsidiary in Ukraine to produce 155mm rounds and spare parts *(June 2024)*.

Chapter 23: Beyond the Battlefield: The Military's Role in Climate Resilience

Dr. Khalid Mahmood **Shafi**, https://orcid.org/0009-0008-5568-694X
Jens Vesterlund **Mathiesen**

Abstract:

Climate change impacts global security by reshaping military strategies, operational efficiency, and infrastructure resilience. Grounded in securitization theory and human security principles, this chapter examines the interplay between military emissions, military vulnerability to climate impacts, and disaster response responsibilities. The study reveals that wartime emissions remain unregulated and underreported, while increasing climate disasters strain military resources. Drawing on cross-national case studies, policy analyses, and climate data, the chapter argues that armed forces must reconcile their dual identities as emitters and responders. By integrating the Knowledge, Attitude, and Practice (KAP) framework, the study proposes institutional reforms to embed climate literacy into military training and decision-making. Furthermore, it advocates for the DIME+E model—combining Diplomacy, Information, Military, Economy, and proactive Environmental stewardship—to address climate security through coordinated national and international action. The study concludes that environmentally conscious military planning is not just good for Earth; it's essential for national security in a changing world.

Keywords: Climate Security, Military Emissions, Operational Adaptation, Sustainable Defense Practices, Disaster Response, Geo-politics

Introduction

Climate change has transcended from scientists and economists to become a critical factor in global security. Initially, it was geologists, climate experts, and financial analysts who flagged climate as a measurable threat to worldwide stability (Babayev, 2024). Military strategists and international relations scholars classify it as a 'threat multiplier', exacerbating pre-existing conflicts and generating new security challenges (Black et al., 2022). Despite all the international talk about climate issues, there is a glaring gap in the conversation: military forces themselves. This oversight needs attention, especially considering the military's dual role as a significant climate contributor and a crucial component of the climate resilience strategy.

Military organizations sit in a contradictory position. While they are essential for security, disaster response, and maintaining political order, they are also massive carbon

emitters and resource consumers (SIPRI, 2024). The United States military is documented as the world's largest institutional energy consumer, emitting over 51 million metric tons of carbon dioxide [CO_2] annually (DOD, 2023). The Pentagon spent $16.5 billion on energy alone, showing just how significant their environmental impact is (Bugos, 2022). Military operations are frequently exempt from emissions targets and climate regulations under national security justifications (UNEP, 2023).

Introducing the 'climate-military nexus' is essential to understanding this relationship better. This concept builds on Jayaram (2020), who argues that militaries are both agents of environmental harm and critical actors in climate resilience. It refers to the bidirectional relationship between climate change and the military, encompassing the military's environmental impact, vulnerability to climate disruptions, and role in climate crisis response (Jayaram, 2020). As an often powerful institutional actor, militaries shape policy directions, influence national priorities, and consume enormous resources that could otherwise support climate adaptation efforts (Schlanger, 2024). With defense spending hitting all-time highs globally, these trade-offs are becoming increasingly stark (Frerks et al., 2024).

The Climate Change Performance Index shows that regions most affected by climate disasters are seeing more military involvement in emergency response (UNDP, 2024). Climate-driven catastrophes like hurricanes and wildfires have dramatically increased military disaster operations (NOAA, 2024). This intersection of climate vulnerability and pollution demonstrates why it is necessary to build climate awareness into defense planning, especially as climate disasters become more severe (IPCC, 2023).

This chapter examines the climate-military nexus through three interconnected lenses: the military's contribution to climate change via emissions, its role in climate-induced disaster response, and the impacts of climate change on military operations and infrastructure. Drawing on cross-national case studies, policy documents, and climate data, the qualitative analysis explores how militaries can transition toward climate resilience while balancing their dual role as contributors to and mitigators of climate risks. By applying the Knowledge, Attitude, and Practice [KAP] framework, the chapter proposes actionable strategies for institutional adaptation. Ultimately, this chapter proposes a holistic framework, the [DIME+E] model (*Diplomacy, Information, Military, Economy, + Environment*) for addressing climate security challenges. This expanded approach recognizes that climate security demands coordinated action across all instruments of national power with a proactive environmental focus.

Theoretical Framework: Climate Change as a Non-Traditional Security Threat

Barry Buzan's *People, States, and Fear* challenges us to think beyond traditional military threats by including environmental and societal dimensions in security studies. His

work questions the standard state-focused security approach by showing how environmental decline and climate shifts threaten global stability (Buzan, 1983).

Scholars like Buzan, Ole Wæver, Richard H. Ullman, and Jessica Tuchman Mathews have collectively pushed for broadening security studies beyond conventional military concerns (Wæver, 2011). Climate change is a non-traditional security threat with diffused adversaries, widespread impacts, and unpredictable consequences. Unlike traditional threats from identifiable adversaries, climate change is global and long-standing and intensifies existing vulnerabilities.

Securitization theory, developed by Buzan and Wæver, explains how climate change is framed as a security threat, necessitating extraordinary measures (Buzan et al., 1998). Similarly, Ullman (1983) argues that environmental degradation and resource scarcity are as destabilizing as military conflicts, as they can lead to state failures, resource wars, and human suffering.

The United Nations Development Programme [UNDP] *Human Development Report* introduced the concept of 'human security', emphasizing that individuals' safety is disrupted by climate change, which affects food security, displaces populations, and intensifies resource conflicts (UNDP, 1994). This perspective stresses the importance of addressing individual security in national and international policies. While these theories offer valuable perspectives on climate change's security implications, they have not completely addressed the military's role within this expanded framework. Some researchers argue to stop treating climate change as just another nontraditional threat and instead recognize it as the central security challenge facing the world today (Baysal & Karakaş, 2017).

By integrating these perspectives, the chapter bridges the gap between theoretical frameworks (e.g., securitization, human security) and the practical realities of the climate-military nexus, offering actionable strategies for institutional adaptation.

Towards a Military-Climate Nexus

Climate change's real-world impact on military operations grows clearer each day. According to research from the Stockholm International Peace Research Institute [SIPRI], climate disasters have doubled over the past thirty years, putting increasing pressure on military forces handling emergency response (Black et al., 2022). The US Department of Defense's [DOD] Climate Change Adaptation Roadmap explicitly identifies that climate change has "significantly disrupted military readiness," which makes operational challenges worse (DOD, 2024). The UK's defense establishment has likewise stated that "Defence must preserve its capabilities despite the impact of climate change" (Defence Committee, 2023).

Despite these acknowledgments showing greater awareness of climate risks in military planning, studies reveal persistent gaps between what military leaders say and what they do.

Many armed forces recognize climate change as a strategic concern on paper but have not developed thorough, systematic approaches to building climate resilience in their operations. Too often, political considerations trump practical operational needs, leaving military organizations underprepared for the full range of climate-related threats they'll face.

The nexus of climate-military geopolitics has evolved into a fragmented global response after the new US administration in January 2025 (CNN, 2025). The reduction in the US National Oceanic and Atmospheric Administration [NOAA] in March 2025 has adversely affected the defense and operational readiness (Zhong et al., 2025). The USA military has notably scrapped existing climate strategies and deprioritized climate terminology in military studies. In April 2025, the Navy Secretary ended the US Navy's 2030 climate action plan, which was issued in 2022. As argued by a Navy spokesperson, the reason for this is: "The Department of the Navy is focused on shipbuilding, deterrence and warfighting. We will no longer be sidetracked by climate-focused decision-making" (Federal News Network, 2025). Further, the US Coast Guard Academy removed explicit references to 'climate change' from its curriculum under new Pentagon directives, signaling a broader policy shift under the 2025 administration (Lavelle, 2025). Meanwhile, European nations and the UK have integrated climate change into national security frameworks, viewing it as a threat multiplier that demands coordinated action (Defence Committee, 2023). However, developing nations of the Global South face a climate paradox in which immediate socioeconomic challenges—poverty, healthcare, and infrastructure—compete for limited resources with climate security.
This chapter explores the climate-military nexus through three key perspectives:

- Military contributions to climate change
- The military as a responder to climate-induced disasters
- Impacts of climate change on military installations, operations, and personnel

The following sections will delve into these perspectives, examining the military's evolving role in climate resilience and the urgent need for institutional adaptation. Rather than sidetracking militaries from warfighting and deterrence, the issue of climate change is, as the following sections will illustrate, an indispensable component of these core tasks.

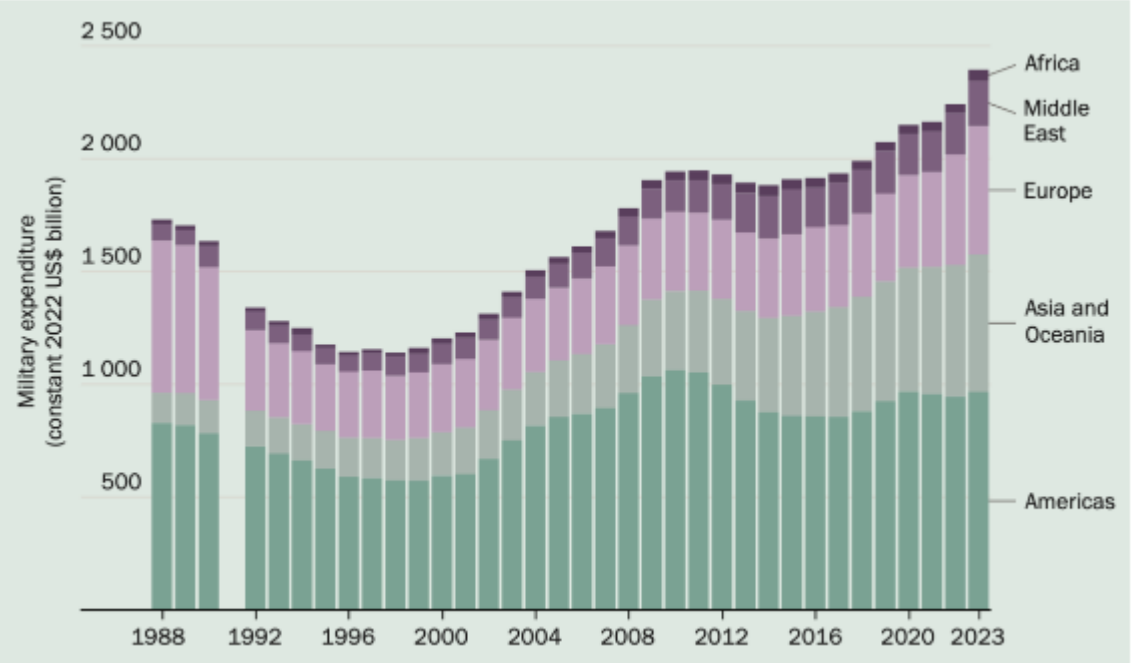
Perspective 1: Military Organizations as Emitters

Militaries worldwide operate extensive fleets of vehicles, naval ships, aircraft, and military infrastructure, consuming vast amounts of fossil fuels and significantly contributing to global carbon emissions. The Conflict and Environment Observatory estimates that global militaries account for approximately 5.5% of total global carbon emissions, surpassing the total emissions of the entire African continent and doubling that of the global aviation industry

(Parkinson & Cottrell, 2022). If military emissions were considered collectively as a single state, they would rank as the fourth-largest emitter worldwide, following China, the US, and India (Parkinson & Cottrell, 2022).

Despite these significant emissions, militaries remain largely unrepresented in global climate agreements (Schlanger, 2024). This omission was cemented in the 1997 Kyoto Protocol, which excluded military emissions reporting. While the 2015 Paris Agreement lifted this exemption, military emissions reporting remains voluntary. Consequently, military climate impact remains severely underreported, as reflected in the United Nations' [UN] *Global Emissions Gap Report 2023*, which acknowledges that military emissions are 'likely nontrivial' but remain 'insufficiently accounted for' (UNEP, 2023). The impact of military carbon emissions is compounded by increased global military expenditures, which reached an all-time high in 2023 as reflected in Figure 23.1.

Figure 23.1: *World Military Expenditure by Region, 1988-2023*



Source: Tian, N., Lopes da Silva, D., Liang, X., & Scarazzato, L. (2024). *Trends in world military expenditure, 2023*. Stockholm International Peace Research Institute (SIPRI). Used with permission. © SIPRI. All rights reserved.

Reporting military emissions remains optional, reflecting an ongoing reluctance to fully integrate military activities into global climate strategies. The report mentions military emissions, acknowledging their likely significance but noting that they remain insufficiently reported (UNEP, 2023). At COP29 in Baku (2024), military emissions were once again absent from the final agreement, despite climate advocates emphasizing that the $300 billion

allocated for climate action is vastly insufficient when compared to the $2.4 trillion in global military expenditures for 2023 (WILPF, 2024).

The US military, the world's largest and most technologically sophisticated armed force, is also the single largest institutional consumer of fossil fuels. The US DOD reported 51 million metric tons of CO_2 emissions in fiscal year 2021, placing it above the national emissions of industrialized countries such as Sweden and Switzerland (Schlanger, 2024). While military organizations do not function as political decision-making bodies, they influence governance significantly, making them key actors in climate mitigation and adaptation efforts (Jayaram, 2020).

The Climate Impact of Warfare

While peacetime military emissions are significant, they do not account for the environmental impact of active conflicts. The Russia-Ukraine war, now in its third year, has generated approximately 175 million metric tons of CO_2, equivalent to the annual emissions of the Netherlands or 90 million cars (Klerk et al., 2024). These emissions stem from:

- The consumption of billions of liters of fuel by military vehicles and aircraft.
- Widespread fires resulting from bombardments and the destruction of infrastructure.
- The heavy use of steel and concrete for fortifications and rebuilding efforts.

The ecological ramifications of warfare extend beyond immediate conflict zones (Crawford, 2019). The destruction of energy infrastructure and industrial facilities has intensified carbon output, with total climate damages from the Russia-Ukraine conflict exceeding $32 billion. Additionally, the closure of Ukrainian and Russian airspace has led to longer commercial flight routes, adding 24 million metric tons of CO_2 to global aviation emissions (Nevitt, 2023).

Bun et al., (2024) emphasize that the climate consequences of conflicts in Ukraine and Gaza extend far beyond warfare's immediate geographic and temporal boundaries, generating long-term ecological disruptions. For example, the Israeli military action in Gaza produced an estimated 420,265-652,552 metric tons of CO_2 in its first 120 days alone, equivalent to burning over 1.5 million barrels of oil (Otu-Larbi et al., 2024). However, existing emissions monitoring frameworks, primarily designed for peacetime industrial and energy sectors, lack the capacity to systematically track wartime emissions, resulting in significant gaps in quantifying their environmental toll (Schlanger, 2024; UNEP, 2023).

As a paper argues, "the climate impact of wars such as those in Ukraine and Gaza extends well beyond the time and place of physical conflict," creating long-term ecological consequences (Bun et al., 2024). Furthermore, existing emission monitoring and reporting

frameworks are not designed to account for wartime emissions, leaving their true impact largely unrecorded (Otu-Larbi et al., 2024).

Perspective 2: Military Deployment as Respondents to Climate-Induced Disasters

The military has historically been involved in disaster response, with its participation increasing significantly since the early 1990s. Notable examples include:

- ***Hurricane Maria in Puerto Rico (2017)*:** The US military conducted one of its most extensive domestic disaster relief operations to restore power, provide medical aid, and transport essential supplies.
- ***Cyclone Idai in Mozambique, Malawi, and Zimbabwe (2019):*** One of the worst tropical cyclones to affect Africa, leading to extensive military-led search and rescue operations and humanitarian assistance.
- ***Australian Bushfires (2019-2020)*:** The Australian Defense Force [ADF] deployed over 3,000 personnel to assist with evacuations, fire containment, and relief efforts.
- ***Pakistan Floods (2022)*:** The Pakistani military played a crucial role in evacuations, relief efforts, and establishing temporary shelters as a third of the country was submerged due to extreme flooding (Shafi, 2022).
- ***California Wildfires (2024)*:** National Guard and active military units were deployed. While military helicopters provided aerial water drops, troops helped with fire line construction, evacuation, and medical aid under joint command structures.

National responses vary, but in most countries, disaster management agencies lead while integrating military and police forces when civilian resources are inadequate. According to the World Bank, by 2050, climate change could displace over 216 million people, escalating the frequency and scale of disasters. This crisis is likely to overwhelm civilian agencies, necessitating expanded military involvement in disaster response (World Bank, 2021).

With increasing climate-induced disasters, militaries are deployed for flood, wildfire, and tsunami relief operations. The US military and National Guard play a significant role in humanitarian assistance, particularly in large-scale disasters such as Hurricane Katrina and California wildfires (Smith, 2023). NATO has similarly integrated climate resilience into its strategic planning, conducting joint exercises and providing humanitarian aid, as seen in the 2019 Eastern European floods. The UN has also explored expanding peacekeeping roles to include climate disaster relief.

Military Disaster Relief in South Asia

South Asia, home to 25% of the global population, is highly vulnerable to climate disasters. The region includes eight of the world's top twenty climate-risk countries, with some of the most polluted cities (Vanzo, 2024). Due to the region's history of conflict and its hosting of two nuclear powers, the military plays a critical role in disaster management.

- ***Bangladesh:*** The armed forces coordinate with the Ministry of Disaster Management and provide humanitarian aid, such as during Cyclone Amphan in 2020 (Tribune, 2020).
- ***Sri Lanka:*** The military has been instrumental in tsunami and flood relief, leading evacuations and rebuilding efforts following Cyclone Ockhi (2017) and the 2020 floods (CFE-DM, 2024).
- ***Pakistan:*** One of the world's most climate-vulnerable nations (UN-Habitat, 2023). The armed forces played a crucial role in the 2010 and 2022 floods, establishing over 200 relief camps and providing food and medical aid as part of their 'Winning Hearts and Minds' strategy (Maddiwale & Virk, 2011). In Karachi's 2015 heatwaves, military units set up relief camps, distributing water and medical supplies (Raza, 2015).
- ***India:*** The Indian armed forces play a vital role in climate disaster response during crises like the 2018 Kerala floods and 2019 Cyclone Fani. The National Disaster Response Force (NDRF), working alongside military units, also conducted over 300 rescue operations during the 2023 Himachal Pradesh landslides (Suri & Sud, 2023).

The military's role in disaster response extends beyond immediate relief, encompassing wildfire suppression, flood mitigation, and early warning systems for glacial lake outburst floods (GLOFs) in mountainous regions. The increasing militarization, i.e., reliance on military forces for climate-related disaster response tasks, underscore its growing importance in climate resilience strategies.

Perspective 3: Effects of Changing Climate on Military Installations, Operations, and Personnel

Global militaries are not only major contributors to carbon emissions and active responders to climate-induced disasters, but their conventional military operations and equipment have also been significantly affected by drastic climate shifts. These changes introduce new challenges, necessitating strategic adjustments.

Historically, severe weather conditions have impacted the effectiveness of armies and, in some cases, altered the outcomes of wars. The unexpected harsh winters in Russia

contributed to the military defeats of Charles XII of Sweden in 1708, Napoleon in 1812, and Hitler in 1941. Such events underscore the critical importance of weather conditions in shaping military strategies. Despite advancements in military technology, climate change continues to strongly influence military preparedness, forcing forces worldwide to adapt their policies and strategies. Drawing from existing literature on military climate adaptation, three key areas where climate change affects military structures and operations have been explained below (Garfin et al., 2021).

Impact on Military Equipment and Platforms

Extreme weather conditions and rising temperatures affect military preparedness and equipment functionality. For instance, at Al Dhafra Air Base in the United Arab Emirates [UAE], where temperatures can soar to 125°F, military aircraft such as the Lockheed Martin F-22 Raptor experience performance degradation. Similarly, high summer heat at Ali Al Salem Air Base in Kuwait has led to the grounding of US Air Force flights and failures in civilian aircraft electronic systems (Sawant, 2023).

At sea, hurricanes and tsunamis pose serious threats to naval installations. In response, aircraft must be moved inland while naval vessels dive deeper into calmer waters. The US military exercises in Fairbanks, Alaska, assess how rising temperatures and environmental shifts affect operational capabilities. These exercises reveal that climate change alters critical factors such as the Time, Space, and Relative Strength [TSR] matrix used in military strategies, affecting deployment efficiency and logistical planning.

China faces similar challenges. The melting of permafrost on the Qinghai-Tibet Plateau threatens military infrastructure, reducing foundation stability and affecting the Qinghai-Tibet Railway, which holds both civilian and military strategic significance. The People's Liberation Army Rocket Force [PLARF] also operates missile bases in permafrost regions, where thawing soil can compromise missile accuracy (Costa et al., 2023).

Impact on Garrisons and Air Bases

Permafrost melt poses severe risks to military bases and energy installations, particularly in Eastern Russia. Former President Dmitry Medvedev warned of the threats to Russian military infrastructure from worsening climate conditions. During a Russian Security Council meeting, he emphasized the need for "thorough checks of civil and military infrastructure in regions with the most complicated climatic conditions" and necessary reinforcement measures (Stoetman et al., 2023).

Military installations, airbases, and garrisons are highly vulnerable to climate-related disruptions. The catastrophic Gayari sector avalanche in the Siachen Glacier, Pakistan (2012), resulted in the loss of 140 soldiers, including a commanding officer, exemplifying the impact

of severe climate events on military personnel (PDMA, 2012). These events highlight the urgent need for resilient infrastructure to ensure operational stability.

Operations and Logistics Challenges

Military operations and logistics face increasing challenges due to climate change. Logistical feasibility determines tactical viability, but maintaining supply routes amid shifting terrain and declining local resources is increasingly difficult.

Another report systematically analyzed climate change's impact on military operations, highlighting vulnerabilities in military readiness and installations. Coastal bases face rising sea levels and tsunamis, while inland bases contend with extreme heat waves and wildfires, disrupting training and maintenance activities. This report illustrates the climate-related risks to military operational capabilities (Congressional Research Service, 2023).

Across South Asia, home to the largest glaciated terrain outside the Poles, the climate creates unique security problems. Take Siachen Glacier—the highest battlefield on Earth—where a staggering 97% of deaths come from harsh weather and altitude conditions rather than enemy fire (Ives, 2004). Examples like this highlight why military planners can't afford to delay incorporating climate adaptation into their strategies.

Pathways for Adaptation and Mitigation

The military troops need systematic strategies to handle these climate challenges head-on. This means building real climate understanding throughout the ranks, shifting mindsets toward sustainability, and implementing workable solutions that reduce vulnerabilities in the field. Climate resilience must be systematically integrated into military training, equipment procurement, and operational planning.

National Response: Integrating Climate Literacy Through the KAP Model

This study proposes integrating climate literacy into military training and operations by applying the Knowledge, Attitude, and Practice [KAP] framework. Initially developed by the World Health Organization [WHO] and widely implemented by UNDP and United Nations Environment Programme [UNEP], the KAP model effectively addresses knowledge and behavior gaps across various domains (Shafi, 2022). To ensure sustained adaptation and mitigation capacity, military institutions must innovate and recalibrate their strategic approaches (Ashbridge & Beard, 2023).

The KAP framework enhances climate literacy within military contexts through three interconnected methodological approaches – knowledge, attitude, and practice.

Building climate-related *knowledge* requires militaries to understand the climate crisis, its effects on military operations, and its broader societal implications. This includes logging

and analysing data on carbon emissions and committing to annual “Climate Budgets” aligned with the Paris Agreement, with full reporting of the carbon footprint across all military activities. The U.S. Department of Defense has already incorporated climate-change education into its training curricula, ensuring that service members receive foundational climate instruction, while programs such as Defense Environmental International Cooperation facilitate knowledge-sharing among allied nations (U.S. DoD, 2019). At the international level, organisations such as UNEP and the UN International Institute for Sustainable Development provide e-training modules to strengthen environmental resource management in UN peace operations, further expanding the knowledge base required for climate-aware military practice.

Cultivating the right *attitude* involves fostering a strong sense of environmental responsibility within military organizations. The British Armed Forces have advanced this effort through awareness campaigns that emphasize reducing carbon footprints and conserving resources, which in turn strengthen morale and reinforce institutional commitment to sustainability (Ashbridge & Beard, 2023). Similarly, the U.S. Marine Corps has revised its training to prepare soldiers for extreme heat conditions, directly acknowledging the growing impact of climate change on military readiness and embedding environmental awareness into operational culture.

Putting sustainable *practice* into action requires militaries to implement environmentally responsible daily operations, including reducing energy consumption and transitioning toward renewable energy sources. The U.S. Department of Defense’s Arctic Mobile Observation System (AMOS) strengthens environmental monitoring in Arctic regions, directly supporting cold-weather operational effectiveness (Langweil, 2023). Similarly, the Royal Australian Navy has revised its supply-chain strategies to remain resilient amid increasing cyclone activity, reflecting the operational pressures of a changing climate (Ide, 2023). At the multilateral level, UNEP has issued policy recommendations aimed at improving environmental performance in peacekeeping missions, ensuring that sustainability and conflict-prevention considerations are embedded in mission planning and execution (Scott & Khan, 2016).

International Cooperation in Addressing the Climate-Military Nexus

Given the transnational nature of climate change, military collaboration across borders is essential, as effective international cooperation strengthens resource-sharing, knowledge exchange, and coordinated crisis-response strategies. The Multinational Military Expert Group, established by the Global Military Advisory Council on Climate Change (GMACCC), fosters intergovernmental dialogue on military climate adaptation (Kingham, 2019), while NATO’s climate-adaptation exercises use alliance-wide simulations to train forces for

climate-induced disasters and humanitarian missions, thereby increasing interoperability among member states (NATO, 2024). At the same time, The United Nations Environment Program (UNEP) works with military forces to integrate climate resilience into UN peacekeeping operations, and future UN Security Council resolutions may increasingly incorporate climate-risk assessments, potentially expanding peacekeeping mandates to address climate-related threats by 2030 (Babayev, 2024). As climate change accelerates, military organizations must proactively adapt, mitigate, and collaborate to navigate the emerging security challenges it creates.

Policy Recommendations

These recommendations aim to reduce military emissions, promote green technologies, and enhance international cooperation to bolster climate resilience within military operations. Integrating climate change into national and international security frameworks is essential for addressing climate-induced threats to military preparedness. Table 1 summarizes key policy recommendations.

Table 23.1:*Summary of Key Policy Recommendations*

Securitizing Climate Change as a Security Threat	Mandatory Military Emissions Reporting
Restructuring Military Organizations for Climate Adaptation	Regional Cooperation and Joint Exercises
Adopting the 6Rs Framework	Increasing Financial Support for Climate Adaptation
Cross-Sector Collaboration	Integrating Climate Resilience in UN Peacekeeping Mandates
Establishing a UNFCCC Military Working Group	The DIME model of climate change

Securitizing Climate Change as a Security Threat

Climate change must be recognized as a top security threat at both national and international levels. This formal acknowledgment would ensure that militaries are better equipped to deal with the risks posed by climate change. By recognizing climate change as an existential security issue, national and international policies can prioritize the integration of climate considerations into military doctrines, making military organizations more proactive in addressing climate-related challenges and conflicts.

Mandatory Military Emissions Reporting

Effective management of military carbon output necessitates mandatory reporting protocols. Military institutions cannot reasonably reduce emissions they fail to quantify, making standardized reporting frameworks an essential prerequisite for meaningful action. The implementation of specialized assessment tools, such as tailpipe emissions methodologies, would enable military organizations to gather precise data, thereby facilitating targeted reduction strategies. This transparency mechanism would simultaneously foster institutional accountability, ensuring military establishments implement progressive measures to diminish their environmental footprint over time (Schlanger, 2024).

Restructuring Military Organizations for Climate Adaptation

Military institutions must fundamentally reconfigure their policies and operational frameworks to incorporate climate considerations. The strategic alignment of military doctrine with climate adaptation and mitigation imperatives will ensure continued operational readiness while simultaneously preparing forces for the anticipated increase in climate-induced disasters that scholarly projections suggest will characterize the near future (Babayev, 2024). While challenging, these institutional transformations represent an essential evolution in military preparedness philosophy that acknowledges the changing security landscape of the twenty-first century.

Regional Cooperation and Joint Exercises

Regional military cooperation is essential for effectively managing cross-border climate crises. Countries' militaries should engage in joint training exercises and collaborative disaster response efforts. Such cooperation enhances resource sharing and ensures coordinated responses during climate-induced emergencies (NOAA, 2024). Mapping the capacities of key regional stakeholders, including military and civilian resources, will ensure that responses are efficient and comprehensive.

Adopting the 6Rs Framework

The military should adopt the 6Rs framework—Realize, Reduce, Reuse, Recycle, Recover, Rest in Nature—to promote sustainability in military operations. The military can reduce its environmental impact and improve operational efficiency by applying responsible resource management principles. This framework encourages long-term environmental stewardship, helping militaries lower their carbon footprints while maintaining readiness for critical operations.

Increasing Financial Support for Climate Adaptation

International financial institutions, such as the IMF and the World Bank, must increase climate adaptation funds for developing nations, earmarking significant portions for strengthening the climate resilience of armed forces. According to the Intergovernmental Panel on Climate Change (IPCC), developing countries will need $127 billion annually by 2030 and $295 billion by 2050 for climate adaptation (IPCC, 2023). However, the current allocation is insufficient, with adaptation funds reaching only $23 billion to $46 billion annually, which accounts for just 4% to 8% of total climate finance (Calvin et al., 2023). Boosting adaptation funds would enable vulnerable nations to enhance their military's climate resilience.

Cross-Sector Collaboration

To address climate challenges comprehensively, militaries should collaborate with other government sectors, academia, industry, and NGOs. Cross-sector partnerships will facilitate the exchange of expertise, resources, and technologies, enabling militaries to adopt more effective climate change mitigation strategies. By pooling resources across sectors, the military can strengthen their capabilities in responding to climate crises.

Integrating Climate Resilience in UN Peacekeeping Mandates

UN peacekeeping missions must incorporate climate resilience into their mandates. This ensures that peacekeepers are not only prepared for conflict but are also equipped to address climate-related challenges. Proactive engagement in climate-induced crises will enhance the effectiveness of peacekeeping forces, promote stability, and prevent resource-based conflicts.

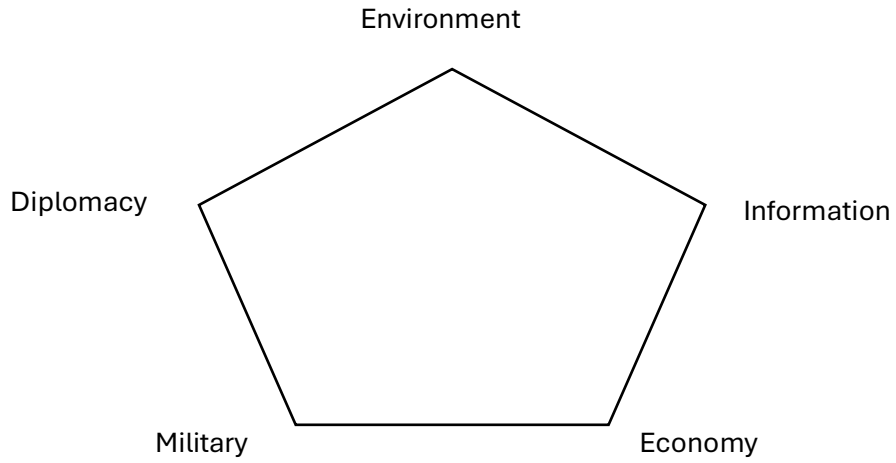
The DIME Model of Climate Change

DIME (Diplomacy, Information, Military, Economy) has long guided national security strategies. While securitization theory frames climate change as an existential threat, and the human security framework prioritizes individual safety from displacement and resource wars, the DIME model overlooks environmental challenges, creating systemic gaps in addressing climate security. Moreover, the climate-military nexus highlights the military's dual role as contributors to climate change and critical actors in climate resilience. This transformation demands an expansion of traditional security frameworks. This study advocates for DIME+E (Diplomacy, Information, Military, Economy, + Environment), explicitly recognizing 'environment' as a distinct yet interconnected challenge with the conventional pillars, as shown in Figure 2. This shift moves beyond treating environmental concerns as a byproduct of military activity to climate security governance.

Each component of the DIME+E framework addresses distinct yet interconnected challenges. Diplomacy fosters multilateral agreements to mandate emissions reporting and

resolve resource-driven conflicts. Information campaigns promote transparency through open-source platforms and counter misinformation about climate threats. Military adaptation includes adopting low-carbon technologies, building climate-resilient infrastructure, and ensuring disaster response preparedness. Economic strategies reallocate defense budgets toward green financing and carbon pricing, balancing security with sustainability. Environmental stewardship demands binding emissions caps. Coordinating action across all DIME+E pillars is essential to adapt national security to a rapidly changing climate.

Figure 23. 2: *DIME+E Model of Climate Military Nexus*



Establishing a UNFCCC Military Working Group

A focused working group within the UNFCCC should be established to facilitate military collaboration on climate resilience (Jayaram & Brisbois, 2021). This group would allow global military forces to share best practices, innovative technologies, and solutions to mitigate the impacts of climate change on military operations.

Conclusion

The climate-military nexus represents the international system's ‘sink or swim’ situation. Global militaries must develop resilience against climate change crises or risk failure if decisive actions are not taken. As climate-induced disasters become more severe and frequent, the military's role as a first responder will continue to expand. Militaries must reassess their bases, platforms, and operational capabilities in the face of extreme weather events.

Armed forces must move beyond traditional strategies by integrating climate literacy through frameworks like the KAP model, embedding environmental stewardship into strategic decision-making and planning. Furthermore, addressing the global impacts of climate change requires international military collaboration to enhance knowledge and develop effective joint strategies (Frerks et al., 2024).

At this pivotal moment, the climate-military nexus demands 'out-of-the-box thinking', emphasizing proactive management of foreseeable challenges while ensuring readiness for unpredictable climate-induced disasters. Addressing the climate-military nexus is a strategic imperative and moral obligation to ensure a secure and resilient future amid growing global uncertainties.

References

Ashbridge, S., &. Beard, A. (2023). Greening defense: The UK armed forces' strategic approach to climate change. *Royal United Services Institute*. https://rusi.org/explore-our-research/publications/commentary/greening-defence-uk-armed-forces-strategic-approach-climate-change

Babayev, M. (2024). Call on climate action for peace, relief, and recovery. *COP 29 Baku Azerbaijan*. https://unfccc.int/sites/default/files/resource/COP29_Letter_to_Parties_and_observers.pdf

Baysal, B., &. Karakaş, U. (2017). Climate change and security: Different perceptions, different approaches. *Uluslararası İlişkiler Dergisi*. 14(54), 21-44

Black, R., Busby, J., Dabelko, G. D., De Coning, C., Maalim, H., McAllister, C., Ndiloseh, M., Smith, D., Alvarado Cóbar, J. F., Barnhoorn, A., Bell, N., Bell-Moran, D., Broek, E., Eberlein, A., Eklöw, K., Faller, J., Gadnert, A., Hegazi, F., Kim, K., … Staudenmann, J. A. (2022). Environment of Peace: Security in a New Era of Risk. In *Black, Richard; Busby, Joshua; Dabelko, Geoffrey D.; De Coning, Cedric; Maalim, Hafsa; McAllister, Claire; Ndiloseh, Melvis; Smith, Dan; Alvarado Cóbar, José Francisco; Barnhoorn, Anniek; Bell, Noah; Bell-Moran, Daniel; Broek, Emilie; Eberlein, Alexis; Eklöw, Karolina; Faller, Jakob; Gadnert, Andrea; Hegazi, Farah; Kim, Kyungmee; Krampe, Florian; ... (2022). Environment of Peace: Security in a New Era of Risk Stockholm: SIPRI - Stockholm International Peace Research Institute 10.55163/LCLS7037 <http://dx.doi.org/10.55163/LCLS7037>* [Info:eu-repo/semantics/report]. Stockholm International Peace Research Institute. https://www.sipri.org/publications/2022/other-publications/environment-peace-security-new-era-risk

Bugos, Shannon. (2022, June). *U.S. Defense Officials Balk at Biden's Nuclear Budget | Arms Control Association*. https://www.armscontrol.org/act/2022-06/news/us-defense-officials-balk-bidens-nuclear-budget

Bun, R., Marland, G., Oda, T., See, L., Puliafito, E., Nahorski, Z., Jonas, M., Kovalyshyn, V., Ialongo, I., Yashchun, O., & Romanchuk, Z. (2024). Tracking unaccounted greenhouse gas emissions due to the war in Ukraine since 2022. *Science of The Total Environment*, *914*, 169879. https://doi.org/10.1016/j.scitotenv.2024.169879

Buzan, B. (1983). *People, states, and fear: The national security problem in international relations*. Wheatsheaf Books Ltd.

Buzan, B., Wæver, O., & Wilde, J. de. (1998). *Security: A New Framework for Analysis*. Lynne Rienner Pub.

Calvin, K., Dasgupta, D., Krinner, G., Mukherji, A., Thorne, P. W., Trisos, C., Romero, J., Aldunce, P., Barrett, K., Blanco, G., Cheung, W. W. L., Connors, S., Denton, F., Diongue-Niang, A., Dodman, D., Garschagen, M., Geden, O., Hayward, B., Jones, C., … Péan, C. (2023). *Climate Change 2023: Synthesis Report* (First). Intergovernmental Panel on Climate Change (IPCC). https://doi.org/10.59327/IPCC/AR6-9789291691647

CFE-DM. (2024). *Sri Lanka: Disaster Management Reference Handbook*. Center for Excellence in Disaster Management & Humanitarian Assistance. https://www.cfe-dmha.org/LinkClick.aspx?fileticket=JcJqafHgiTU%3d&portalid=0

CNN. (2025, March 7). *Officials and experts warn that Pentagon plans to cut climate programs will hurt national security*. https://edition.cnn.com/2025/03/09/politics/pentagon-climate-cuts-national-security

Congressional Research Service. (2023). *U.S. military and climate change: A review of current adaptation and mitigation strategies* (No. IF12161). https://crsreports.congress.gov/product/pdf/IF/IF12161

Costa, R. T. da, Krausmann, E., & Hadjisavvas, C. (2023). *Impacts of climate change on defense-related critical energy infrastructure*. Publications Office of the European Union. https://eda.europa.eu/docs/default-source/brochures/climate-report.pdf

Crawford, N. C. (2019). Pentagon fuel use, climate change, and the costs of war. *Costs of War*, 1–46.

Defence Committee. (2023). First Special Report: Defence and climate change (First Special Report of Session 2023–24). *House of Commons*. https://publications.parliament.uk/pa/cm5804/cmselect/cmdfence/32/report.html

DOD. (2023). *Department of Defense Plan to Reduce Greenhouse Gas Emissions*. Office of the Under Secretary of Defense for Acquisition and Sustainment. https://media.defense.gov/2023/Jun/16/2003243454/-1/-1/1/2023-DOD-PLAN-TO-REDUCE-GREENHOUSE-GAS-EMISSIONS.PDF

DOD. (2024). *Department of Defense Climate Adaptation Plan 2024-2027*. Department of Defense, Office of the Undersecretary of Defense (Acquisition and Sustainment).

Federal News Network. (2025). *Navy Secretary John Phelan ends climate action plan as DoD cuts program*s. https://federalnewsnetwork.com/defense-main/2025/04/navy-secretary-john-phelan-ends-climate-action-plan-as-dod-cuts-programs/

Frerks, G., Geertsma, R., Klomp, J., & Middendorp, T. (Eds.). (2024). *Climate Security and the Military: Concepts, Strategies and Partnerships*. Leiden University Press. https://doi.org/10.24415/9789087284381

Garfin, G., Falk, D. A., O'Connor, C. D., Jacobs, K., Sagarin, R. D., Haverland, A. C., Haworth, A., Baglee, A., Weiss, J., Overpeck, J., & Zuñiga-Terán, A. A. (2021). A new mission: Mainstreaming climate adaptation in the US Department of Defense. *Climate Services*, *22*, 100230. https://doi.org/10.1016/j.cliser.2021.100230

Ide, T. (2023). Climate change and Australia's national security. *Australian Journal of International Affairs*, *77*(1), 26–44. https://doi.org/10.1080/10357718.2023.2170978

IPCC. (2023). *Intergovernmental Panel on Climate Change*. Intergovernmental Panel on Climate Change. https://www.ipcc.ch/report/ar6/wg1/

Ives, J. (2004). *Himalayan perceptions: Environmental change and the well-being of mountain peoples*. Routledge. https://www.routledge.com/Himalayan-Perceptions-Environmental-Change-and-the-Well-Being-of-Mountain-Peoples/Ives/p/book/9781138867130

Jayaram, D. (2020). 'Climatizing' military strategy? A case study of the Indian armed forces. *International Politics*, *58*, 619–639.

Jayaram, D., & Brisbois, M. C. (2021). Aiding or undermining? The military as an emergent actor in global climate governance. *Earth System Governance*, *9*, 1–5. https://doi.org/10.1016/j.esg.2021.100107

Kingham, R. A. (2019). *The climate security nexus: Implications for the military*. Global Military Advisory Council on Climate Change. https://www.envirosecurity.org/news-archives/the-climate-security-nexus-implications-for-the-military

Klerk, L. de, Shlapak, M., Gassan-zade, O., Korthuis, A., Zibtsev, S., Myroniuk, V., Soshenskyi, O., Vasylyshyn, R., Krakovska, S., & Kryshtop, L. (2024, June 13). *Climate damage caused by the Russian war in Ukraine in 24 months*. Ukraine Recovery Conference 2024, Berlin. https://climatefocus.com/wp-content/uploads/2024/06/Climate-damage-caused-by-russian-war-in-Ukraine-in-24-months.pdf

Langweil, M. (2023, October 26). *Armed forces work to adapt to a changing climate*. U.S. Army. https://www.army.mil/article/271203/armed_forces_work_to_adapt_to_a_changing_climate

Lavelle, M. (2025, March 7). US Coast Guard Academy Censors 'Climate Change' From Its Curriculum—Inside Climate News. *Inside Climate News*. https://perma.cc/8MJY-VZMM

Maddiwale, A., & Virk, K. (2011). Civil-military relations in natural disasters: A case study of the 2010 Pakistan floods. *International Review of the Red Cross*, *93*(884), 1085–1105.

NATO. (2024). *Climate security: Impacts on NATO's operations and strategies*. NATO HQ. https://www.nato.int/nato_static_fl2014/assets/pdf/2024/7/pdf/240709-Climate-Security-Impact.pdf

Nevitt, M. (2023). Environmental War, Climate Security, and the Russia-Ukraine Crisis. *Ohio St. LJ*. 84, 1359

NOAA. (2024). *Billion-dollar disasters: Climate-driven emergencies on the rise*. National Oceanic and Atmospheric Administration.

Otu-Larbi, F., Neimark, B., Bigger, P., Cottrell, L., & Larbi, R. (2024). A Multitemporal Snapshot of Greenhouse Gas Emissions from the Israel-Gaza Conflict. *Social Science Research Network*.

Parkinson, Dr. S., & Cottrell, L. (2022). *Estimating the Military's Global Greenhouse Gas Emissions*. Scientists for Global Responsibility (SGR) and the Conflict and Environment Observatory (CEOBS). https://ceobs.org/wp-content/uploads/2022/11/SGR-CEOBS_Estimating_Global_MIlitary_GHG_Emissions.pdf

PDMA. (2012, April 7). *Siachen Avalanche*. https://pdma.punjab.gov.pk/siachen_avalanche

Raza, A. (2015). National disaster management authority in Pakistan: Role of Pakistan army in disaster management. *Journal of Social and Administrative Science*, *2*(1).

Shafi, K. M. (2022). *Now or never: Realizing global green regime—UN, Pakistan climate crisis*. Discover STM Publishing. https://discoverpublish.com/un-pakistan-climate-crisis/

Sawant, M. (2023). Expeditions with MCUP: Weather – The only constant in warfare. *Marine Corps University Press*. https://www.usmcu.edu/Outreach/Marine-Corps-University-Press/Expeditions-with-MCUP-digital-journal/Weather/

Schlanger, Z. (2024). Military emissions are too big to ignore. *The Atlantic*. https://www.theatlantic.com/science/archive/2024/01/military-emissions-climate-cop28/677151/

Scott, S., & Khan, S. (2016). The implications of climate change for the military and conflict prevention, including through peace missions. *ASPJ Africa & Francophonie*, *3*(7). https://www.airuniversity.af.edu/Portals/10/ASPJ_French/journals_E/Volume-07_Issue-3/scottkhan_e.pdf

SIPRI. (2024). *SIPRI Yearbook 2024: Armaments, Disarmament and International Security*. Oxford University Press. https://global.oup.com/academic/product/sipri-yearbook-2024-9780198930570?cc=pk&lang=en&

Smith, T. (2023). Amid the hurricane and wildfire seasons of 2023, service members found a shoulder to lean on with the USO. *United Service Organizations*. https://www.uso.org/stories/3640-amid-the-hurricane-and-wildfire-seasons-of-2023-service-members-found-a-shoulder-to-lean-on-with-the-uso

Stoetman, A., Zandee, D., Dams, T., Drost, N., & van Schaik, L. (2023). *Military capabilities affected by climate change: An analysis of China, Russia and the United States*. Clingendael Institute. https://www.clingendael.org/sites/default/files/2023-01/Military_capabilities_affected_by_climate_change.pdf

Suri, M., & Sud, V. (2023, August 15). Himachal Pradesh flooding: People trapped under a collapsed temple as heavy rains kill more than 60. *CNN*. https://edition.cnn.com/2023/08/14/asia/india-himachal-pradesh-trapped-temple-rain-climate-intl/index.html

Tian, N., Lopes da Silva, D. ,. Liang, X. ,. &. Scarazzato, L. (2024). Trends in world military expenditure, 2023. *Stockholm International Peace Research Institute*.

Tribune, D. (2020, May 21). Cyclone Amphan: Armed Forces begin post-disaster activities in affected areas. *Dhaka Tribune*. https://www.dhakatribune.com/bangladesh/210604/cyclone-amphan-armed-forces-begin-post-disaster

UNDP. (1994). *Human Development Report 1994: New Dimensions of Human Security*. United Nations Development Programme.

UNDP. (2024). *The Peoples' Climate Vote 2024: Results*. United Nations Development Programme.

UNEP. (2023). *Emissions gap report 2023*. United Nations Environment Programme. https://www.unep.org/resources/emissions-gap-report-2023

UN-Habitat. (2023). Country report 2023. *United Nations Human Settlements Programme*. https://unhabitat.org

U.S. DoD. (2019). *Report on effects of a changing climate to the Department of defense*.

Vanzo, T. (2024). Top cities with the worst air pollution. *Smart Air Filters*. https://smartairfilters.com/en/blog/top-cities-worst-air-pollution/

Wæver, O. (2011). Politics, security, theory. *Security Dialogue*, *42(4-5)*.

WILPF. (2024). *COP29 in review: Failures, progress, and what's next?* Women's International League for Peace and Freedom. https://www.wilpf.org/cop29-in-review-failures-progress-and-whats-next/

World Bank. (2021). Groundswell: Preparing for internal climate migration (Updated). *World Bank Group*. https://www.worldbank.org/en/news/feature/2021-groundswell-report

Zhong, R., Gaffney, A., & Flavelle, R. (2025, March 8). More NOAA Employees May Be Let Go, Making 20% of Staff Cut—The New York Times. *The New York Times*. https://www.nytimes.com/2025/03/08/climate/noaa-layoffs-trump.html

Chapter 24: Force Multipliers: Providing Quality Advice to Defence and Security Stakeholders

Dr. Harry **Kowal**, Brigadier-General (Retired), CD
Andre **Dupuis**, Colonel (Retired), CD, OMM

Abstract:

The COVID-19 pandemic gave way to an unprecedented number of retirements and resignations globally. This was not good news for the Canadian Armed Forces (CAF), which was already struggling with not only retaining the force but also recruiting new members. Both the loss and lack of experience make it extremely challenging for decision- and policy-makers to deal with the complexities of today's security environment and plan for the future. Over the years, civilian companies have learned to harness knowledge and experience in Defence and Security. One such Canadian company is Space Strategies Consulting Ltd [SSCL], which has been providing advice to the Defence and Security community for many years. In keeping with the theme of the ISMS Conference 2024 "Scaling Up, Learning Lessons, Ensuring Quality," this paper offers insight into the fine-tuned SSCL process, which may serve as a model for others.

Keywords: Defence, Security, National Security, Space Strategies Consulting Limited [SSCL], policy advice, concept advice, ensuring quality, learning lessons

Introduction

Today's security environment continues to be threatened by state and non-state actors whose actions are challenging the international order, leveraging technology like never before and showcasing global reach. As articulated in Canada's latest Defence Policy and Defence Policy Update, Canada, once comforted by distance and geography, understands full well the importance of modernizing defence capabilities because of its vulnerability to global threats as well as those posed by the opening of the Arctic due to climate change (Government of Canada, 2017; Government of Canada, 2024).

But what a challenging time for scaling up, modernizing and re-building, expanding educational programs, re-evaluating doctrine and generating the force. On the heels of the COVID-19 pandemic, countless organizations experienced a considerable reduction in their workforce, a mass departure that has been coined the 'Great Resignation' (Klotz, 2021). In the US alone, "…47 million people quit in 2021, and 50 million more in 2022, according to data from the US Bureau of Labor Statistics [BLS]" (Morgan, 2023). In Canada, the Canadian Armed Forces [CAF] is experiencing significant recruitment and retention challenges of its own (Government of Canada, 2022). It is one of the biggest issues facing the new Chief of the

Defence Staff [CDS], General Jennie Carrignan, with predictions from her predecessor that problems "…are going are get worse before they get better" (Brewster & Raycraft, 2022). This is grim news for Canada, which recently published its Defence Policy Update that re-affirms its commitment to supporting domestic and global security and announces a substantial investment in defence spending (Government of Canada, 2024). There is little doubt that both the lack and the loss of experience makes it extremely difficult for decision- and policy-makers to navigate the complexities of today's global Defence and Security environment, let alone chart a vision for a better tomorrow.

Given internal resources challenges, decision and policy-makers reach outside their organization to seek advice to help meet their requirements. There are numerous civilian companies that have stepped up to meet that demand, each with their own methodology in support of their clients. One such Canadian company, Space Strategies Consulting Ltd [SSCL], has many years of experience providing advice for their clientele. In keeping with the theme of the ISMS Conference 2024 "Scaling Up, Learning Lessons, Ensuring Quality," this paper presents the SSCL process to offer insight into their methodology as an example of how they are responding to needs of the Defence and Security community.

Total Defence

Expanding contributions to defence and security from outside of government departments can be a significant force-multiplier. As explained by Sundelius and Eldeblad (2023), a Whole-of-Society perspective on defence and security is inclusive of all stakeholders from government and non-government agencies to private corporations and individuals. "Doing more with less may be less of a challenge if more stakeholders are contributing to the effort" (Sundelius & Eldeblad, 2023, p. 96). While their research highlights the importance of the preparedness of individuals, the perspective of this paper hones in on the importance of leveraging the expertise and experience of the right mix of individuals. While it was true that talent and experience left in droves as a result of the pandemic, research has also shown that this was short lived. It has been reported that, on the heels of the Great Resignation, came something that has been referred to as the Great Re-shuffle, suggesting that people still wanted to work, but that they needed either something more fulfilling or ways to contribute on their own terms. In 2023, the BBC reported on data analyzed from ZipRecruiter that showed the massive amount of reshuffling and, given the circumstances post pandemic, suggested that it was a "one time" event (Morgan, 2023). In other words, people have likely settled into what they moved away from and are now ready to re-engage. This is opportunity and from a whole-of-society perspective, this workforce can be very beneficial in fulfilling the demands for experience and expertise to ensure quality advice is provided to Defence and Security Stakeholders.

Effective Teams

Having resources available is not a solution on its own. Building the right team is absolutely critical to producing quality output. Forbes, for example, reports: “By building diverse workforces, organizations can propel innovation, improve company decision-making and create an engaging and supportive work environment” (Miller, 2023). In fact, there has been a substantial amount of research in Canada that speaks to the benefits of equity, diversity and inclusion [EDI] in mobilizing the full spectrum of ideas, talent and experiences that are needed for innovation and creativity (UnivCan, 2016). In 2017, Universities Canada published its commitment to EDI through Inclusive Excellence Principles to “recognize the vital importance of a diversity of identity and thought, with room for a variety of ideas, geographies, cultures and views” (UnivCan, 2017).

In terms of subject matter expertise, David Epstein discusses the advantages that generalists can have over specialists. While also underscoring the importance of diversity, he advocates for engaging a broad range of experience, offering that it is difficult for specialists to imagine solutions outside their narrow specialization (Epstein, 2019). By involving generalists and those with less experience, there is an added benefit to the processing the information. When those with less experience or those who are generalists are involved, they tend to ask the kinds of questions that specialists may take for granted as being obvious. The result is the kind of reflection that leads to better understanding and better content in what is being produced.

SSCL Approach

SSCL has been serving the Security and Defence community for well over a decade (SSCL, n.d.). With the breath of advice, they have provided dozens of clients, a lot can be learned from how they do business. They are mission-focus on bringing forward innovative solutions to even the most complex challenges, employing small, diverse and multi-disciplinary teams to address security and defence issues. Over the years, they have built upon their expertise in air and space to take a pan-domain approach to problem-solving that includes all elements of National Security impacted continually by the rapidly evolving global environments. SSCL has learned that not only is it essential to bring together the right team to leverage experience and expertise but also that the way information is gathered and processed is critically important to achieving desired outcomes.

Project success at SSCL is not just about delivering on time and within budget. SSCL’s goal is to build lasting partnerships by ensuring that every stakeholder is engaged, aligned, and invested throughout the process, ultimately leading to client satisfaction. Stakeholder engagement is extremely important because every project involves a variety of players from

clients, contractors, corporate agencies, internal teams, and external partners, each with their own opinions and perspectives. Without a structured approach, there can be misalignment of expectations, unclear objectives, delays and even missed opportunities. Accordingly, the SSCL process integrates stakeholder engagement into every phase of the project, ensuring all voices are heard, requirements are understood, and challenges are addressed. At SSCL, the integration of everyone involved in the project is the responsibility of the Program Management Office [PMO] and the Project Leader [PL], both of whom are appointed for each project. The SSCL process is broken down into phases as follows:

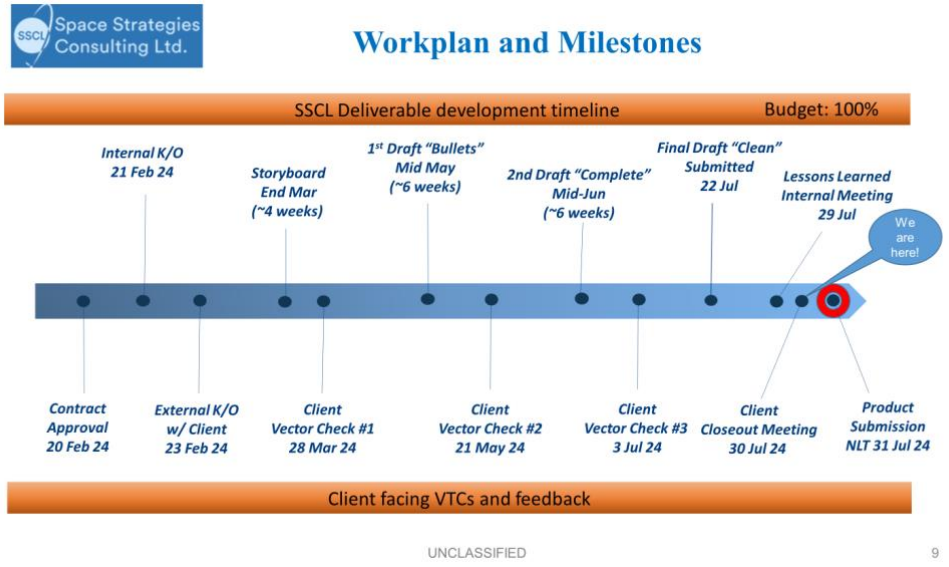
Initial Support Estimate [ISE]

During this initial phase, all key stakeholders are identified, including clients, agencies, and project contributors, to gain a sound understanding of their roles and expectations. This way stakeholder engagement can be tailored according to their impact on the project. The project scope is also defined during ISE so that objectives, deliverables, and key milestones can be best understood, ensuring everyone is on the same page before execution begins.

It is during the ISE phase that the Project Team is established. The PL is selected by the SSCL executive through a call for interest. The PMO in collaboration with the PL then selects the members of the Team. In addition to the PL and PMO, a typical project team includes a variety of Writers, Researchers and a Senior Reviewer. The number of Writers and Research depends on the magnitude and complexity of the project but one of the writers is always a Technical Writer to ensure the quality and standardization of the documents produced. Note that, while having subject matter experts involved in each project is essential, project teams at SSCL are established to ensure the participation of generalists and those less experienced. In addition, SSCL recognizes the intrinsic benefits of having diverse teams and strives to ensure full spectrum of ideas, talent and experiences is leveraged.

The result of the ISE is the workplan, which is put together initially by the PMO and the PL but is then finalized through collaboration with the Project Team and the client. In addition to breaking down the project into level of effort expected for each team member, the workplan outlines the milestones for each project. Figure 1 is a typical SSCL Workplan and Milestones, which showcases the structured engagement from project initiation to project closeout. The Workplan is reviewed periodically through the process to ensure a common understanding among team members and with the client and to facilitate responsiveness and adaptability. During the ISE, internal and external kickoff meetings are held to ensure expectations are clear and that the workflow to achieve results can be executed seamlessly.

Figure 24.1: *Typical SSCL Workplan*



Source: (SSCL, n.d.)

Read-in

The Read-in phase is important for collecting feedback and data to refine operational and technical needs before project development begins. During this phase, the Project Team gathers information, such as key references, and initiates their research. A typical process will include a brainstorming session to collaboratively shape a Storyboard. The Storyboard is SSCL's way of expressing the approach to be taken to present the deliverable, which typically culminates in the development of the outline for the document being created. During the Read-in phase, the Team also puts together Requests for Information (RFIs) that are submitted to the client. RFIs can lead to access to references and technical specifications. They are critical to ensuring a common understanding of requirements and are also cost effective since the Team is not spending valuable time researching information that the client may have quick access to. The RFIs are also another way to better understand stakeholder involvement and whether or not other Subject Matter Experts (SMEs) need to be involved in the project.

Project Execution

This phase of the process can vary from project to project in that there are different approaches that a Team can choose to tackle the work, each approach as unique as the members of the Team themselves. What is consistent during this phase is that the Storyboard, which serves as the foundation of the deliverable, is transformed into various draft documents, starting with ideas captured in bullet form. Over time, these bullets points lead to draft paragraphs which lead to a finished product that contains all the research and references for a robust discussion followed by conclusions and recommendations. Typical products range

from strategic concepts, concepts of operations/employment and statements of capability deficiencies to discussion papers, doctrine and lessons learned, to name a few.

Throughout the execution phase, progress of work is tracked regularly through weekly or biweekly check-ins. These meetings are ongoing touchpoints that help keep the project moving in the right direction and serve to identify and address any issue proactively. In addition to these Team meetings, monthly reports are also completed and sent to the client to provide transparency to the process and insights into deliverables, timelines, and budget. Change is inevitable with any project and is factored into the SSCL process so that scope shifts, technical challenges and funding changes are addressed as quickly as possible. To this end, SSCL uses the “Vector Check”, which is scheduled multiple times throughout the execution phase. These are client engagement meetings that serve as stakeholder review sessions to validate project outputs and ensure alignment with expectations before finalizing deliverables. As there are multiple Vector Checks scheduled throughout project execution, refinements to the deliverables are, therefore, iterative in nature, taking stakeholder feedback and incorporating it before project submission. Vector Checks prevent costly rework and misalignment and are instrumental to achieving client satisfaction.

Project Closeout

The final phase of the SSCL process is Project Closure, which culminates with the submission of deliverables and represents project completion. During this phase, SSCL holds internal lessons learned sessions, providing the opportunity for the Team to reflect on the work accomplished, to highlight what went right and what could have been done better and to explore how future projects can improve. As a learning organization, SSCL has embedded lessons learned into its process because it allows them to grow and evolve. Improvements to the SSCL process has been achieved by leveraging digital tools for real-time project tracking, enhancing knowledge-sharing across the company and other subsidiaries, aligning with best practices to drive efficiency and strengthening collaboration with industry partners. For each project, lessons learned are shared with the client at the closeout session at the end of the contract. They are equally valuable, however, to new Project Leaders, who are required to read them in advance of their project so that these are truly lessons learned and not just lessons recorded. This final phase of the SSCL process includes a Project Closure meeting, which is an opportunity for SSCL to receive feedback from the client. Equally important, it is also an opportunity for SSCL and the client to reflect on the deliverables and the process and to discuss refinements that can be made.

Conclusion

The Defence and Security strategic landscape continues to be very challenging and especially so due to resource shortfalls. To fill the void, decision and policy-makers seek outside help, leveraging contributions from contractors to serve as force multipliers. The reshuffling of people post-pandemic indicates that there are resources available to provide experience and expertise to the Defence and Security community. In fact, there are many companies from which to choose, each with their own methodology in supporting their clientele. This paper provides insight, however, into the approach taken by SSCL, a Canadian company, which has executed and refined their process over many years of providing advice to Defence and Security stakeholders.

The process used by SSCL is but one example of various approaches that are taken by contractors; however, much can be learned by examining the SSCL process that can help decision and policy-makers ensure they are receiving the highest quality advice. At SSCL, projects are tackled by small, diverse and multi-disciplinary teams to address security and defence issues. They use a structured methodology to ensure there is alignment of expectations and a clear understanding of objectives. Their strategic approach to stakeholder engagement is based on collaboration, clear communication and adaptability from start to finish, which is enacted through a series of RFIs, Vector Checks, and milestone reports, keeping stakeholders informed and ensuring clients' needs and concerns are addressed. As a learning organization, SSCL also has embedded lessons learned into its process, which are shared with the client and within the company and which have enabled them to grow and evolve.

Building the right team is critical to cultivating the innovative and creativity that is essential in producing the best outcomes. Whether engaging with a contractor or working through a problem on your own, a structured process can be immensely beneficial for producing the best results. With the right process, you can have the confidence to deliver successfully time and time again. It is important, however, to be willing to listen and learn so that whatever process is used can evolve and improve. Continuous improvement built into the process will also facilitate the opportunity of leveraging experience from one project to another, one team to another or one company to another. Given the information presented in the article and the likelihood for contractors to be engaged as force multipliers in the future, it would be interesting as follow-on research to explore and compare other processes to investigate "best practices" that decision and policy-makers should come to expect as they reach out for quality advice.

References

Epstein, D., (2019). Range: Why Generalists Triumph in a Specialized World. Riverhead Books. ISBN: 9780735214484 (ISBN10: 0735214484)

Government of Canada. (2024). *Our North, Strong and Free: A renewed Vision for Canada's Defence*. Ottawa: Department of National Defence. https://www.canada.ca/content/dam/dnd-mdn/documents/corporate/reports-publications/2024/north-strong-free-2024.pdf

Government of Canada. (2017). *Strong, Secure, Engaged – Canada's Defence Policy*. Ottawa: Department of National Defence. https://www.canada.ca/en/department-national-defence/corporate/reports-publications/canada-defence-policy.html

Government of Canada. (2022). *Report of the Standing Committee on National Defence: Modernizing Recruitment and Retention in the Canadian Armed Forces*. House of Commons online. https://publications.gc.ca/collections/collection_2022/parl/xc34-1/XC34-1-1-441-2-eng.pdf. Pg 22.

Klotz A. 2021. The Covid Vaccine Means a Return to Work and a Wave of Resignations. Think: Opinion, Analysis, Essays. NBC News Digital. https://bit.ly/3Hg9PWL

Brewster, M., & Raycraft, R. (2022, October 6). *Military personnel shortage will get worse before it gets better, top soldier says | CBC News*. CBCnews. https://www.cbc.ca/news/politics/eyre-shortage-directive-1.6608107

Miller, J., (2023, August 16). The Power Of Diversity And Inclusion: Driving Innovation And Success, *Forbes*. https://www.forbes.com/councils/forbesbusinesscouncil/2023/08/16/the-power-of-diversity-and-inclusion-driving-innovation-and-success/

Morgan, K. (2023, August 2). *The great resignation is "over."* BBC News. https://www.bbc.com/worklife/article/20230731-the-great-resignation-is-over-what-does-that-mean

Space Strategies Consulting Ltd. (SSCL). https://www.sscl.solutions/ and https://www.linkedin.com/search/results/all/?fetchDeterministicClustersOnly=true&heroEntityKey=urn%3Ali%3Aorganization%3A64724502&keywords=space%20strategies%20consulting%20ltd&origin=RICH_QUERY_SUGGESTION&position=0&searchId=9bb4df8e-072d-415e-af9a-1865e89fd474&sid=Dpw&spellCorrectionEnabled=false

Sundelius, B., & Eldeblad J., (2023). Societal Security and Total Defense: The Swedish Way National Defense University Press. *PRISM Vol. 10, No. 2*. https://ndupress.ndu.edu/Media/News/News-Article-View/Article/3323928/societal-security-and-total-defense-the-swedish-way/

Universities Canada (UnivCan). (2016) *Mobilizing people and ideas: Supporting the creative economy and fostering Canadian culture in the digital world*. https://univcan.ca/wp-content/uploads/2016/12/universities-canadas-submission-to-the-consulations-on-canadian-content-in-a-digital-world-november-2016accessible-1.pdf

Universities Canada (UnivCan). (2017) *Principles on equity, diversity and inclusion*. https://univcan.ca/news/universities-canada-principles-equity-diversity-inclusion/

Chapter 25: Unlocking Policy Performance with Organisational Innovation – Public-Private Partnerships' Potential for Grand Strategy Designs

Megghi **Pengili**, Ph.D.[1], ORCID: https://orcid.org/0000-0002-7218-799X

Abstract:

The issue of defence transformation is becoming even more pertinent given the entangled geopolitical climate. The ongoing war on Ukraine, the conflicts in the Middle East as well as the Red Sea crisis, strategic competition and the illicit use of disruptive technologies attacking critical infrastructures have all increased the intensity and scale of hybrid threats and asymmetric domains of conflict. These strategic circumstances require defence establishments to continue adapting by building effective partnerships with the defence industry. These public-private partnerships (PPPs) are as much institutional as they are procurement entities and therefore have the potential to design the future security contexts for the designers' advantage by inducing defence organisations into learning processes. This work examines the potential of PPPs to enable defence organisations to design a grand strategy of defence by exploring how defence organisations create preferred conceptualisations and employ tactics for making grand strategy utilising knowledge. To this purpose, the analysis is structured around a tripartite approach focusing on knowledge management–organisational learning-–organisational change (since design is a choice for change) (Buchanan, 2008). Informed by the case studies of Italian and Israeli PPPs in the cyber and aerospace sectors, this qualitative analysis is developed on the theory of dynamic institutional change. Besides contributions to the studies of military design and defence strategy, this analysis makes a practical contribution to security consulting.

Key words: public-private partnerships, defence transformation, organisational innovation, grand strategy designs, Italy, Israel

Introduction

The modernisation and transformation of defence go hand in hand. This means that the production or acquisition of advanced technologies for the armed forces is grounded in the organisational decision to design operational concepts that alter the conduct of the conflict. Importantly, design is different from routine planning. While systematic planning signifies mobilising existent resources in today's operational framework, design concerns visionary knowledge that creates new resources to transform future security contexts (Zweibelson,

[1] Views are my own and not those of the University of Leeds.

2023, pp. 20–22). In other words, design is about knowledge assets through which defence organisations learn to innovate.

Effective organisational learning is a collective process grounded in the expertise of government-industry partnerships, since the emergence of new technological systems in the digital space, in 2010, blurred the boundaries between policymakers and industry entrepreneurs and required the defence organisation to learn how to institutionalise an open innovation approach (Merindol & Versailles, 2020). This moment marks the transition from defence industrial bases to defence innovation ecosystem (Merindol & Versailles, 2020). These innovation ecosystems are run by public private partnerships [PPPs] that are engaged with either the critical study or the strategic and operational application of heterogenous expertise in the interest of national security.

The strategic environment of the next decade will be very different from what it looks like now or what it was in the past. The ongoing war on Ukraine (2022–), the Hamas attack on Israel in 2023, and potential proxy wars between the USA and China with potential battlefields in Venezuela or Myanmar (Tierney, 2021) exemplify this. Against this backdrop, governments are pushing the defence sector to go beyond its remit of reactive defence towards proactive defence. This attitude is also reflected in the publications developed by both the Italian and Israeli governments in the period between 2017–2022 – the two case studies of this paper (Belfer Center, 2015; Technion Haifa, 2017; Eisenkot & Siboni, 2019; Ministero della Difesa, 2021a, 2021b, 2022a, 2022b, 2022c). Both Israeli and Italian strategic publications reflect the institutional efforts in these countries to build a posture of excellence through a set of grand objectives. This set of goals mobilises the defence industry and its specific connection with the military by coordinating actions, resources, and emerging actors in order to:[2]

- create an awareness to adapt and transform as a response to systemic challenges.
- establish participatory governance with defence industry actors to support and inform defence planning.
- harmonise the activity of the parallel educational programmes run by the defence industry and institutions and to encourage the circulation of personnel from both sectors to identify talent.
- create synergies with the industry to develop niche projects.
- contribute to strengthening the national and multinational defence industrial base
- foster innovation diplomacy, leveraging PPP's expertise.

[2] See more on the recent developments to include partnerships and organisational learning in defence at: 2024 Security Cooperation Conference: Building Lasting Partnerships: What Have We Learned? at: https://dscu.edu/bgcy-ralli/sc-conference24 accessed on 27 August 2024

In other words, partnerships are being deployed as a way of problem-solving that seeks to control risk and maximise the chances of success during the application of power in the pursuit of an objective suggesting, thus, a new strategic era. This era has brought in new decision-making actors and the need for a new strategic thinking to design the future security context. While current literature is worried about PPP's performance in technological innovation, the defence community is continuously engaging PPPs to increase organisational resilience to win the next wars by operationalising specialised knowledge.

The activity of PPPs in this paper suggests that developping a grand strategy for defence should not rely on a static view of ends, ways and means. As regards our case studies, Italy does not have a written national grand strategy because there's no government white book, according to Admiral (Rt) Giampaolo di Paola (2021).3 As a consequence, in the absence of a national grand strategy and a defence grand strategy, Italy is married to the EU's and NATO's raison d'être (Ministero della Difesa, 2021c, 2022b, 2022d). As outlined in the Strategic Concept of the Italian Chief of Defence (2022c), defence grand strategy is conceptualised as an organising principle and a plan. Therefore, in the case of Italy, grand strategy is about frameworks, guidelines, commitments, and policy actions that consolidate the country's foreign policy and proclaim the country's loyalty to NATO and the EU (Ministero della Difesa, 2021b). This, also, signifies that Italy's grand principles and plans are framed topdown according to international commitments and directives.

Differently from Italy, Israel's grand strategy is driven around a core military doctrine based on four pillars: deterrence, early warning, decisive victory, and protection. The lack of a written document is mainly explained by Israel's strategic culture that is prone to improvisation and constant adaptation (Barak et al., 2021). Eitan Shamir likewise asserts that: 'In the unending turmoil of the Middle East, even five-year plans are soon overtaken by events, so that many if not most multi-year programs require many changes and adaptations (2019, p. 17). The academic literature also describes Israel's culture as being prone to an improvisational style over more structured long-term planning. Israel's national strategy could therefore be described as grand behaviour (Silove, 2018) shared between the valence of 'domestic issues and the urgent need to respond to security and diplomatic challenges'

[3] The interviews included in this chapter are part of the PhD thesis of the author, 4 Feb 2024, for which access is embargoed since it will be turned into a book. Copyright understandings implies that this information is copyright material and that no quotation from these interviews may be published without proper acknowledgment. The data that support the findings are available from the corresponding author (M.P) upon reasonable request. Own summarising and translation from the Author's interview with Admiral Giampaolo Di Paola (Rtd), former Minister of Defence, former Chief of Staff, former Chairman of the NATO Military Group (5 October 2021, Italy): "Ma …innanzi tutto perché la difesa può creare una Grand Strategy, ci vuole una Grand Strategy Nazionale. Cosa che in Italia, una Grand Strategy nazionale non é mai stata fatta quello che si chiama una Grand Strategy. Un libro bianco del governo, non il libro bianco della difesa…. Poi a discesa dal libro bianco viene quello della difesa… il libro bianco che é un documento che viene puntualmente, regolamento aggiornato…quella e la Grand Strategy nazionale …ed é quello che poi discendono in cascata diciamo il libro bianco della difesa, la Defence Strategy. Il problema é che in Italia in effetti non c' é mai stato un libro bianco nazionale, non esiste. "

(Shamir, 2019, p. 217). Israel's grand strategy has been characterised more by continuity than change. However, the events of 7 October 2023 will require defence strategists to (a) identify change rather than continuity, (b) work on those capabilities that translate the four pillars of the doctrine the right way to achieve national strategc goals, and (c) evaluate how organisational and technological innovation in peace and wartime works differently across all forces.

On this basis, it is possible to draw some reflections which will guide the goal and structure of this paper. From a big picture perspective, the rise of cooperative advantages or PPPs (Arquilla & Ronfeldt, 1999, p. 35) have brought in new actors, governance dynamics, and the need to reconceptualise grand strategy towards or through the power of knowledge and ideas. In this new strategic era, national interests are PPP-driven. PPPs are not only a critical military-technological innovation strategy but also increasingly part of many countries' strategic efforts to remain competitive and become proactive (Evron & Bitzinger, 2023, p. 218). That said, how best to make a grand strategy for defence remains, thus, a contested subject (Howard, 2001, p. 2).

The paper is structured as follows. After the introduction, Section One explores the variety of PPPs in defence. Section Two establishes a theoretical-conceptual frame around PPP's potential for organisational change and therefore grand strategy designs by applying the approach 'knowledge management–organisational learning–organisational innovation' around the dynamic institutional change theory.4 Building on that frame, Section Three engages practical examples to observe PPP's activity in cyber and aerospace sectors in Italy and Israel applying the analysis on two learning levels, individual and community learning. Indicators generated from each learning level will feed the summary in table 3 illustrating PPPs' contribution to grand designs. Section Four discusses the downsides of public-private collaborations. Conclusions reflect potential areas to explore quantitatively and qualitatively.

PPPs: definitions, scope, and forms

The term public-private partnership [PPPs] originated in the 1970s and is associated in part with the rise of the rhetoric of the specifically neoliberal free market (Department of Economic & Social Affairs- UN, 2016). PPPs began entering public sector governance structures from 1990 (Kappeler & Nemoz, 2010), as an alternative approach for governments to gain access to private capital and obtain financial support for projects in construction, transport, and welfare services (Cavelty & Sute, 2009). Since then, governments and, later, international organisations have made wide use of these partnerships to handle issues that

[4] "The theory emphasizes the role of entrepreneurial actors in identifying innovative institutional solutions and their ability to forge supportive political coalitions for their adoption" (Andonova, 2017, p.34)

require more than an institutional response. This preference towards PPPs rather than creating a new government agency lies with several factors, such as governmental budgetary issues, level of expertise, cost-efficiency issues, and divergence among institutional preferences (Hodge & Greve, 2005; Andonova, 2017, pp. 44–49). In epistemological terms, there is no definition of PPPs.

Cooperation between the public and private sectors can be understood in multiple, overlapping ways: it may be product- or service-oriented (Ham & Koppenjan, 2001, cited in Hodge & Greve, 2005); it can reflect a "culture of engagement" (Sedjari, 2004, p. 303); it may take the form of organisational identity (Haque, 2004); or it can be understood as a type of institution (Andonova, 2006). More comprehensively, the UNECE and Greve & Hodge (2016, p. 3) describe public–private cooperation as potentially representing a specific project, a management tool or organisational form, a policy instrument, a governance tool, or an historical and cultural context—illustrating the conceptual breadth and institutional diversity that characterise contemporary public–private partnerships.

Besides these, an additional concept of PPPs is that of defence entrepreneurship – branded by James Hasik – which draws on the partnership entrepreneurial capability to hunt for and adopt novel solutions under uncertainty generating organisational changes in defence (Hasik, 2016, pp. 113–114). These partnerships are defined as collaborative arrangements between the public and private, whereby combining knowledge, expertise, and assets with the private sectors help the army generate new resources and reassess the nation's own national power (RAND Corporation, 1999).

The absence of a unified definition of the public-private partnership, besides the variety of PPP, is also influenced by the evolution of the partnership. From a project facilitator to a policy tool, the PPP ended up as a knowledge management ecosystem. To make sense of this evolution, the complexity theory lends us the concept of emergence (Turner & Baker, 2019). According to this concept, emergence in systems involves causation and causality, with simple systems relying on reliable, uniform, predictable, and controlled relationships, while complex systems like defence organizations face unpredictability (Zweibelson, 2022).

With regard to their scope, PPPs in defence come in a variety of forms which allows for their extended application for business profits and organisational strategic goals (Kapilashrami, 2010; Andonova, 2017; Wojewnik-Filipkowska & Wegrzyn, 2019; NATO Science &Technological Organisation, 2019). At the same time, to increase access to resources and knowledge for organisational change, PPPs are employed as joint institutional ventures [IJVs] (Hall, 2008), to create synergies between experts for the production of organisational knowledge for a purposeful action.

PPPs scope of operation is also extended to state-owned enterprises [SOEs]. As hybrid creations of economics and politics, SOEs have always played important roles in the

political economies of nation-states (Hodge & Greve, 2005, p. 8), since they dispose the resources, expertise, and connections to forge a state's interests in military modernisation. SOEs operate similarly to private enterprises and also can take advantage of certain characteristics of public ownership to foster innovation, since their activity is defined by uncertainty. This circumstance might discourage private initiatives, such as small and medium enterprises [SMEs], and justify the role of the public sector as an entrepreneur in activities related to new technologies. All these three forms – PPPs, IJVs and SOEs – are built on public-private contractual collaboration – although with different arrangements in terms of governance and autonomy (Hodge & Greve, 2005, p. 8; Castro & Janssens, 2011; OECD, 2024, p. 14; Sánchez-Carreira, Vence, & Rodil-Marzábal, 2020).

In conclusion, PPPs can improve military culture by (a) engineering the competitive context for innovation and (b) creating career paths for talent, while preserving enduring organisational values (Hill, 2015). However, for the defence organisations to recognise the value of knowledge and the appreciation of its practitioners requires a cultural change which continues to be the most difficult for the military to assimilate. To mitigate this issue, the theoretical account below suggests that PPPs engage in designing knowledge management structures and programs which aim to contribute to the transformation process in defence to achieve its strategic edge.

Theorising PPPs' Contribution in Defence Grand Design

'The theory of dynamic institutional change challenges the state-centric and international bureaucracy-focused perspectives' on institutional change (Andonova, Governance Entrepreneurs, 2017, p. 34). These approaches consider either states or international agencies as the main principals behind the establishment of new institutional forms or the institutional adaptation of standard procedures (Andonova, 2017). Instead, dynamic institutional change emphasises the rise of entrepreneurial actors who in times of crisis identify innovative solutions and ensure their adoption through expert support such as the case of the Leonardo Cyber Academy. This Academy's programmes are integrated with defence educational programmes on partnership platforms between defence institutions and Leonardo defence industry in order to provide skills for military and civilian personnel to face threats to national security.

To better locate the contribution of PPPs for grand strategy designs, the theory suggests the application of epistemic infrastructure – which is understood in this analysis as an advanced form of the epistemic community. The epistemic infrastructure inherits the notion of episteme from Foucault (1970), as well as the definitions of John G. Ruggie (1975, p. 569) and Peter Haas (1990, p. 2) of 'epistemic communities'. Conceptualised as epistemic infrastructure, PPPs operate across orders of knowledge and governance by connecting micro

and macro levels of expertise through the PPP's tools and structures (Littoz-Monnet, 2017). The PPP's performance is explained through the division of knowledge resources among experts and the benefits that the PPP brings to the organisation. For example, in the case of Israel, the blurred borders between the civilian and the military, the common strategic culture explained with the security context which Israel affords, along with the shared repertoire for innovation create multimodal platforms that favour social learning amongst defence experts (Sheffer & Barak, 2013). These insights suggest that Israeli PPPs have the authority to formulate policy solutions (Sheffer & Barak, 2013) to the benefit of its security community (Apostolakis & Smith, 2003; Andonova, 2006).

A PPP's authority is expressed in its functionality as a policy and norm entrepreneur while 'taking risks and promoting new designs for problem-solving strategies' (Andonova, 2017, p. 22). As a result, the PPP creates legitimate knowledge upon which defence establishments build their decisions. Subsequently, the 'importance of a PPP, as epistemic infrastructure, becomes vital as it transforms the political governance into epistemic governance' (Carayannis, et al., 2012, pp. 174–175). In other words, PPPs become the drivers for organisational strategic actions to achieve an organisation's long-term goals (Andonova, 2017, p. 11) (i.e., to craft grand strategy)

The literature observes a prescriptive and a causal interpretation of grand strategy distributed along three strategic shifts. The first shift concerns political-military dynamics; the second shift is mainly economic, and the third emerging is the intensification of the information revolution (Arquilla & Ronfeldt, 1999), with its implications that knowledge is power. The following is a brief discussion of these understandings of grand strategy, and the Italian and Israeli interpretation of them in order to support our argument about the strategic importance of PPPs.

As prescriptive interpretation, grand strategy suggests a plan of actions which previews the use of all available political, military, and economic resources to win the war (Freeman, 2021). Prescriptive definitions are provided by Robert Art, Barry Posen, John Lewis Gaddis, Edward Luttwak, Paul Kennedy and Sven Biscop. Art thinks that grand strategy 'concentrates on how the military instrument can best be used to support foreign policy goals' (2009, p. 1). Posen, meanwhile, portrays grand strategy as 'a state's theory about how it can best "cause" security for itself' (1984, p. 1). Gaddis states that grand strategy is 'the alignment of potentially unlimited aspirations with necessarily limited capabilities' (Gaddis, 2018, p. 12). Luttwak, though, avows that grand strategy is 'the level of final results (2001). This is also the everyday form of strategy, because the dynamic workings of the paradoxical logic are constantly present in international politics, even when war in any form is only a highly theoretical possibility' (2001, p. 207). Kennedy considers grand strategy to be 'about the evolution and integration of policies that should operate for decades, or even centuries' (1991,

p. 4), and Biscop frames grand strategy ‘under the heading of ten criteria for action: simple, competitive, creative, comprehensive, rational, allied, agile, courageous, dirty, and proactive’ (2021, p. 3). All these definitions provided above share the absence of a focus: either resource or information.

The causal interpretations of grand strategy on the other hand are resource- and knowledge-focused. In terms of resources, Clive Jones (2022), in the overture to The conceptualisation of grand strategy and the Middle East, questions the influence that dual-use technologies have had in shaping grand strategy and to what extent this is the case (2022, p. 9). He justly refers to the example of cyber and Israel’s instrumentalisation of its technological excellence to build bilateral relationships with countries in the region (Jones, 2022, p. 9). Thierry Balzacq and Simon Reich explain that ‘the goal of a grand strategy is to articulate a state’s guiding beliefs, values and priorities, and to establish coherence and consistency in a state’s behaviour’ (Balzacq, Dombrowski, & Reich, 2019). In a similar vein, Hal Brands and Peter Layton converge in their belief that grand strategy is a specific type of decision-making process, a methodology used by policymakers to solve problems (Brands, 2012; Layton, 2018), which, according to Brands, ‘involves figuring out how to align today’s initiatives with tomorrow’s desired end-state’ (2014, p. 1).

The third and last shift on which interpretations of Grand Strategy are distributed, focuses on the adaptation of statecraft to the information age. David Ronfeldt and John Arquilla developed the term *noopolitik* to interpret the significance of knowledge for grand strategy.5 They state that: ‘Strategy from a noopolitik perspective will be more about identifying, assessing, and affecting peoples’ understandings’ (Ronfeldt & Arquilla, 2021, p. 16). This implies that changes in an individual's beliefs and behaviors can influence the collective mindset of a culture and society. Among the trends inviting noopolitik are the cooperative advantages, which ‘strengthen the capacity of state and nonstate actors to work together to address transnational problems’ (Arquila & Ronfeldt, 1999, p. 35). This trend is already pronounced in the efforts of institutions and defence industry actors to build PPPs for a competitive defence ecosystem.

Within the frame of these interpretations, it is important to meditate briefly on the relationship between military doctrine and grand strategy. From an institutional perspective, Deborah Avant notes ‘a relative integration of grand strategy and military doctrine as the fundamental determinant of how military doctrine influences the security of a state’ (1993, p. 411). As the case of Israel exemplifies, it is the military doctrine that drives grand strategy (Echevarria, 2017, pp. 7–17). This circumstance is explained with the strong relationship between the political-military and operational factors and elements (Ben-Horin & Posen,

[5] *Noopolitik* is a combination of the Greek words νόος (nóos) meaning intellect, or ways of knowing, and πολιτικός (politikós).

1981). Grand strategy as a function of military doctrine can bring advantages and disadvantages. In the case of Israel, advantages can be attributed to the fact that 'to maintain the security status quo through a shift in balance beteween deffence and offence components' (Barak, Sheniak, & Shapira, 2021, p. 2). With regards to disadvantages, the war on Gaza showed that Israeli military doctrine faced challenges which in turn spilled over into the vision and objectives of the country's conceptualisations for grand strategy. The analysis of Eran Ortal in Israel's First Total War identifies three factors which contributed to the derailment of Israel's strategy: 'short sighted policy, overrelliance on sophisticated technology, and failure to adapt to a new set of military threats within the correct framework of Israeli defense strategy' (Ortal, 2024). All these reflections on grand strategy and doctrine will also be the focus of analysis of the next section.

Analysing PPPs in building Grand Strategic Designs – Individual and Community Learning in the Italian and Israeli Partnerships

As an emerging governance actor, the PPP mobilises the internal capacity of defence organisations by injecting stimuli and learning from the external environment in which these organisations find themselves (Andonova 2017, p. 54). Thus, before delving in to the empirical illustrations of the case studies, it is necessary to create a link between grand design dimensions and organisational changes. In other words, how do PPPs design a vision, a plan for the defence organisation when accidents can be expected due to asymmetric threats and the complexity of the operations they involve?

The breadth of the strategic context where Italian and Israeli defence industries operate, speaks to how the industry seeks through its expertise to align with and sometimes also shape national strategic objectives and foreign policy goals. To defence organisations the relationship between industry and institutional partners can be key to the performance and the endurance of the entire organisation when the latter must compete with the better opportunities to build capacities to tackle challenges. This fact explains why public-private partnerships a major issue of discussion and concern for the role they are playing in defence transformation.

The empirical evidence informed by Israeli and the Italian cases applied at two learning levels, individual and community. The various techniques employed to collect and analyse the data, encompass anthropological, neuroscientific, and qualitative research methods combining primary and secondary sources. Such a combination of approaches was necessary when researching in a complex setting that "calls for enhanced sensibility regarding the nuances and degree of access" (Garsten & Nyqvist, 2013, p.45). This access cannot be obtained through organisational charts of the defence organisations—which are both a puzzle and a problem in terms of information content. It is a puzzle as through which formal and

informal channels (i.e. not official communication) knowledge circulates across organisational hierarchies, and a problem because little is referred to in terms of individuals' skills, experience, or qualifications, which are important in appreciating individual's role to organisational knowledge.

Nevertheless, the collection of data met some limitations. These limitations are broken down into three distinct groups. The first group covers the pandemic period (2021-2022) in which empirical evidence was collected, the second group concerns the methods applied to collect and analyse data, while the third group deals with institutional constraints and secrecy in the field. The author mitigated both issues because of their former professional background and the culture sensitivity towards defence and security institutions.

Organisational innovation is determined by how its members learn either individually or in community (group), and therefore the starting point when building the conceptual framework is to consider OI through the prism of these learning levels. Second, it is assumed that the defence ecosystem and/or policy governs, 6 the organisational/institutional learning (strategic), 7 PPPs (systematic), and single experts (technical). To connect the theory of dynamic institutional change with the analysis and the concepts, these learning levels (strategic, systematic, and technical) correspond to the three levels of institutional influence/change: regulative (organisational), normative (community), and cognitive (individual). Third, we establish the stock and flow of knowledge as essential components of the KM capability of a PPP. While stock here corresponds to the accumulated knowledge that resides within these learning levels, flow indicates the amount of knowledge which is transferred between people and across the three learning levels to formulate those activities that enable innovations in the institutions, governance, and policy strategy. Given this, we are allowed to think that PPPs foster four grand designs through the utilisation of specialised knowledge. First, as system integrators placed within the defence ecosystem, the partnerships are responsible for bringing together borderless expertise which adds to the leadership of tomorrow. Second, PPPs induce institutional proliferation within defence institutions in order to increase internal resilience. Third, PPPs, by processing specialised knowledge, are positioning defence towards future-oriented thinking and, as a result, towards anticipatory governance. In other words, they are equipping decision-making structures with the ability to learn, prepare, recognise, and manage future challenges (Klein, et al., 2007 as cited in B & Pezzulo, 2011). Fourth, they define the model of defence innovation ecosystem to envision the future of the defence policy, since defence policy frequently communicates its vison through innovation processes. (see Table 3)

[6] Interchangeable terms for the study's purpose.
[7] *Refer to* note 3

Case Study One: Leonardo Cyber Academy and Axon Ventures Capital [VC]

The analysis here invokes two distinct case studies, namely the PPPs run from the Leonardo Cyber Academy (Italy) and Axon Venture Capital (Israel). The first is located in the cyber industry and the second more broadly on digital technologies and talent recruitment. Combining cyber and digital technologies with institutions helps us understand how PPPs induce institutions to think out of the box to enhance their resilience.

Changes start from where ideas are born, namely in the abilities, expertise, and conceptual thinking of the given organisation's members. Therefore, organisational learning depends mainly on individuals' tacit knowledge and capability to learn (Kucharska & Erickson, 2023), and vice versa, organisational characteristics can drive or hamper individual learning. For instance, if the organisation has a culture conducive to collective learning and knowledge sharing, this encourages individual learning within the PPP (Bennet & Bennet, 2004). These reflections form the background of the individual level of analysis.

Scholarship has applied several models in an attempt to capture individual learning and make sense of Knowledge Management [KM] activities. Mary Crossan, et al., (1999) held that community and organisational learning start at the individual level through intuition and the interpretation of information; this occurs in two ways: bottom-up and top-down. Crossan's model, however, seems to ignore the influence of conscious awareness while placing a greater emphasis on learning and the role of the individual as an agent of influence (Cohen, 2016). In the case of Axon VC, the founders, Talpiot graduates, set out with a clear objective to fund and support the projects of Talpiot alumni (Axon VC, 2019). Here, the consciousness element steers the venture capital activity: the founders identified Talpiot alumni as the best targets through which to achieve and implement their goals by influencing others in their community and rallying them to get behind the founders' cause. Axon VC, as a Talpiot-led company, have the resources to connect with the university's programme and know exactly what students like to do after completing the programme. Offering to support Talpiot start up initiatives, Axon VC ensures that talent does not drain and that the best technologies remain in the country and at the service of defence (Interview between the Author and Rear Adm (Rtd)Ophir Shoham, Axon VC, 2021).8 The second process in Crossan et al.'s model is interpretation, through which information is articulated (1999, p. 525). Anne S. Huff (1990 as cited in Castaneda and Rios, 2007) suggests that individuals develop cognitive maps based on their context and that these maps affect what part of the context is selected and interpreted. This concept is compatible with the principles of Albert Bandura's social cognitive theory, where learning occurs through dynamic and reciprocal interaction between a person, the environment, and human's

[8] The interviews included in this chapter are part of the PhD thesis of the author, 4 Feb 2024, for which access is embargoed since it will be turned into a book. Copyright understandings implies that this information is copyright material and that no quotation from these interviews may be published without proper acknowledgment. The data that support the findings are available from the corresponding author (M.P) upon reasonable request.

behaviour (Bandura, 1965). According to this social cognitive theory, and similar to Bourdieu's ideas, individuals are reactive and proactive to situations (1990). In particular, they develop knowledge to predict the consequences of actions to formulate goals in an anticipatory manner (Castaneda & Rios, 2007), reaching the crest of the wave as agents of innovation (Haas, 1990). The theory of dynamic institutional change refers to these agents as 'entrepreneurs who are able to spot problems innovatively, prepared to take risks and promote innovative approaches to the problem solving. These entrepreneurs have the ability to organise others to help turn policy ideas into organisational policies' (Andonova, Governance Entrepreneurs, 2017, p. 22-23).

For instance, while the decision to launch Leonardo's Cyber & Security Academy was bottom-up, for Axon VC it was top-down – which seems to invert the usual patterns of practice in both countries. The latter's founders are also its leaders. Arik Czerniak, one of Axon VC's three founders, graduated as a fighter pilot from Talpiot, majoring in maths, physics, and computer science. One of his niche projects was to create a website providing psychometric, psychological, and professional testing to filter out the best candidates for a job (Kanon, 2008). This online recruiment service grew out of Czerniak's need for adequate staff for his own ventures. Therefore, he decided to establish a company focused on building a community of trained talents. The essential function of a visionary leader is to model desired behaviour, communicate the organisation's vision and strategy, and insist on the effective implementation of relevant policies and procedures (Bennet & Bennet, 2004). As Czerniak's case reflects, leadership learning encourages the development of knowledge by making one's tacit knowledge available to others.

Besides leadership teaching, another aspect of learning at the individual level that has gained prominence in the literature is setting up micro labs which serve to create and capture knowledge for innovation. Peter Senge and John D. Sterman (1990) introduced the concept of micro labs as the loci in which understandings and strategies would be shared and modified, thus representing a key competitive advantage. Leonardo's Cyber & Security Academy was born out of a micro lab, with the support and contribution of Leonardo Global Solutions [LGS]. At the centre of its activity, LGS recruits skilled employees through initiatives promoting an aptitude for change through the strengthening of expertise (Leonardo, 2022a).

According to Stefano Bordi, Senior Vice President at the Cyber & Security Solutions Division at Leonardo, the number of students that have graduated from the Academy has already reached 5,000 with over 300 courses available in various fields, provided at both the national and international levels (Olio, 2022; Leonardo, 2022b). The Academy's objective is to build institutional cyber resilience for defence organisations since cyber is not only a matter of computer science; living in a cyber society, cyber culture, and cyber economy requires a

holistic approach to the study of cyber, especially in defence where a threat can come from all these factors.

Cyber Academy shows that by sharing a common organisational culture towards organisational change to envision a grand strategy, Leonardo's knowledge workers and leadership were able to identify which information was needed and how quickly it should be applied. This highlights the difference between learning and knowledge processes. While knowledge creation, sharing, and storage may be assumed to be similar in general, successful learning processes are mostly local and depend upon the individual learning stock or their existing capital of information, the environment and culture, as well as, in this particular case, Leonardo's structure and technological instruments.

This implies that organisational characteristics are fundamental if not decisive for individual learning and to the innovation process in general. A fundamental prerequisite for individual learning is a suitable attitude and the motivation of the individual knowledge workers. In this case, the LGS is part of a structure where knowledge managers may influence individuals' attitudes and motivation towards innovation. With that in mind, structure and leadership seem to support individual learning through the effective nurturing of the necessary culture, infrastructure, technology, policies, and behaviour creating, as such, favourable conditions for the individual to learn about their organisation and also create knowledge that contributes to organisational growth.

In both cases discussed here, it is inferred that innovation starts with individual learning, which occurs either in micro labs within the organisation or is built upon the individual's previous experience and their inclination to explore more. In the case of the Cyber & Security Academy, the individual learning stock is built from life-learning within Leonardo itself or from cross-project learning. Meanwhile, at Axon VC, individual learning is isomorphic: leaders, members, and clients all come from the same strategic, cultural, and educational background and thus share similar attitudes towards innovation. Rather than treating it as a barrier, Axon VC uses isomorphism to build on the equilibrium between expertise development and knowledge processes. By inter-hiring between similar bodies, people from the same educational backgrounds will approach problems in much the same way, and therefore, socialisation on the job reinforces these conformities (DiMaggio & Walter Powell, 1983).

Table 1 summarises this case on how individuals within the PPPs learn and perform to defence grand strategy designs by encompassing the relationship between knowledge management and individual learning to enforce institutional capacities. From left to right, column 1 comprises the organisational resources or capabilities (i.e., technology, culture, expertise). These organisational resources support the development of knowledge capabilities (column 2) that drive individual learning and determine its efficiency or performance (column 3). Both, knowledge development and individual learning are

conditioned by factors that hamper their flow (column 4) and those that promote these activities (column 5).

Table 25.1: *Knowledge Development and Individual Learning Expertise*

Organisational Capability	Capability Indicators & Knowledge Development	Efficiency of Individual Learning	Inhibitors for Knowledge Development & Learning Efficiency	Drivers for Knowledge Development & Learning Efficiency
Technology	Individuals are provided with/create their own information technology Individuals have access to efficient and modern technology	Understanding	NA	All capability indicators
Structure	Individuals develop knowledge in compliance with the organisation's vision Individuals are organised into expert units as per their area of expertise to develop expertise Individuals are trained and supported	Development of competencies Translation of expertise into novel ideas and action	Bureaucracy Censored information from the organisation	Trained and supported individuals Career support
Culture	Individuals reflect the culture of their community of experts Individuals are stimulated to feed new knowledge from external and internal sources into the organisation	Growth of expert networks	Lack of emotions Lack of intellectualism Monopolisation of information	Motivation
Expertise	Individuals identify what knowledge needs to be developed and how Individuals learn constantly Individuals have learning skills Individuals know how to develop knowledge across projects or from a variety of resources Individuals are interested in consolidating their own knowledge	Conscious awareness through cross-learning	Lack of expertise	Individuals learn constantly about new knowledge and expert networks Project resources utilised by the individuals to learn Individuals are interested to consolidate their expertise by linking previous knowledge to new information

Continues on the next page...

Information	Information and data are accessible and available in many forms to the individuals Systematic storages are available for knowledge development		Information inaccessibility	Existing database and information in the organisation are relevant to the individuals' need for efficient use
Environment	Individuals compete constructively for knowledge Individuals learn how to mitigate barriers to information Individuals are motivated to learn		Competition for knowledge	Reflective learning

Source: *Developed by the Author, 2024 based upon Aujirapongan et al. 2010 and Bontis et al., 2002*

Case Study Two: PPPs in the Italian Aerospace Sector – the International Flight Training School

The Italian defence community did not officially recognise its partnerships with particular industries until 2021, with the first Multiannual Defence Planning Programme (2021–2023) followed by a second plan covering the period of 2022–2024 (Ministero della Difesa, 2021b; 2022a). Other strategic documents released between 2021 and 2023, such as the Strategic Concept of the Chief of Defence, the Directive for Industrial Policy (2021) and the National Military Policy Directive (2022), paid significant attention to the inclusion of traditional and other industries in the defence ecosystem.

Notwithstanding Italy's internal political dynamics, there is little doubt that its allies and partners at the EU and NATO consider the Italian defence industry as a pillar of excellence, renowned for its reliability and innovation, as demonstrated in various bilateral and multilateral initiatives regarding the aerospace sector in particular (Braw, 2022). In this context, the transformation and modernisation of the Italian Armed Forces take precedence. The Pluriannual Document of 2022–2024 (Ministero della Difesa, 2022a) allocates a significant investment of €18 billion to both processes with a long-term goal to reach 2 per cent GDP at NATO level (Battaglia, 2022). The 216 projects listed in the Pluriannual Document 2022–2024 engage a cluster of industries in designing ambitious programs in light of the country's need to secure its values and interests in new and more determined ways in the increasingly volatile context of current international affairs (Ministero della Difesa, 2022a). An example of these programmes is the International Flight Training School [IFTS], pioneered and managed by Leonardo. The IFTS is a partnership project run by the Italian Air Force and Leonardo. The Air Force's experience, combined with Leonardo's advanced technology, allows for pilots to be trained for sixth-generation fighter aircrafts in the most complex operational scenarios.

The first generation of these pilots graduated in 2022 with the curriculum co-designed by Qatar, Germany, Singapore, and Japan (Madeddu, 2022). The IFTS is a programme of very high strategic value, allowing for, once fully operational, the creation of an innovative flight training centre. (Leonardo, 2022a; Madeddu, 2022). Sadly, neither Leonardo's nor the Italian Ministry of Defence's [MoD] website provide detailed data about the activity of this community-level partnership between the Italian Air Force and the Leonardo defence company. Nevertheless, the existing information allows us to deduce that IFTS is an investment in Italy's foreign policy and the country's interests as a G7 member in terms of country's strategic partnerships in the energy, shipbuilding, and defence sector (The Peninsula Qatar, 2023). Also, cooperation with Singapore and Japan confirms Italy's growing interests in the Indo-Pacific especially after the war on Ukraine, 'confirming a new political, economic, and military activism featured Italian foreign and defence policy in this region' (Coticchia and di Celso, 2024, p. 2). As regards Germany, besides commitments in NATO and the EU, in November

2023, Giorgia Meloni and Olaf Schulz committed, from 2024, to running an annual bilateral forum on the policies of European industrial strategy and strategic industries (EESC, 2012; Agenzia Nova, 2023; EEAS, 2023).

Further, the case study of the ITFS informs us that by navigating Italy's foreign policy goals and the economic interests of the state and industry, the military learns how to align their actions and resources for their imemdiate interests by becoming part of the bigger picture of Italy's idea/vision for grand strategy. This suggests that in the IFTS case, the military and industry learn through the project itself. Project learning allows for the discovery of new knowledge by combining individual knowledge stocks and the information that the external events contribute. Information gathered through Open Source Intelligence [OSINT] allows us to deduce that, to achieve organisational learning from the project learning, goals should be general and not specific (Ken, 2003). In this case, IFTS goals are made uniform through knowledge exchange between the community and the organisation, and then transformed into rules and codes for the community at the project level to deliver an organisational change (Drinkuth et al., 2001, pp. 447–449).

Last, the IFTS 's case study reveals a PPP involved in defence diplomacy (often referred as defence engagement now)9 (Cottey & Forster, 2004, pp. 15-30). Lech Drab defines 'defence diplomacy, as the co-formation and implementation of the state security policy, by creating stable, long-term international relations in the field of defence' (2018, p. 57). IFTS, as these observations show, conducts defence diplomacy through a dynamic strategy which combines: innovative technology, foresight in training fighter pilots for the next jet generations, multilateral cooperation, and transfer of expertise to its international partners such as Qatar, Japan, Germany, Singapore, Austria, Canada, UK, and Sweden (Leonardo, nd).

Case Study Three: PPPs in the Israeli Aerospace Sector – the Israel Aerospace Industries (IAI) activity

While in Italy, community learning is part of a whole-of-government approach, known as Sistema Paese, which serves to consolidate Italy's influence in world affairs, Israeli PPPs, instead, rely heavily on technological innovations to maintain or establish allies and nurture strategic relationships. Israeli defence industry actors always seek to be the first to identify technologies' characteristics and exploit their potential, which is leveraged by Israel to develop dependent relationships with countries in need of Israeli equipment, thereby preserving strategic friendly ties (Rodman, 2005).

Israel Aerospace Industries [IAI] was founded in 1953. The company is the largest in Israel and has delivered technologies and systems in all domains (sea, air, land, space and

[9] "…an instrument for attempting to build cooperative relations with former or potential adversaries and thereby helping to prevent potential conflicts." (Cottey & Forster, 2004, p. 16)

cyber) (IAI, nd). IAI's activity is supported by its four subsidiaries: ELTA Systems, Systems Missiles and Space, Military Aircraft, and Aviation (IAI, nd). As any state-owned enterprise, IAI, too, has been using the PPP model to invest in projects with business and public bodies by 'linking the private and public in important ways' (Hodge & Greve, 2005, pp. 8-29). With that in mind, in IAI, the Israeli government is the sponsor or enabler of the very businesses from which it receives defence equipment, material, and services. This hints at the symbiotic relationship between the state and defence businesses beyond the conventional dynamics of the marketplace and reinforces the view of the state–defence industry relationship as one that is complicated and susceptible (Heidenkamp, Louth, & Taylor, 2013). That the Israeli government finds it appropriate or necessary to sponsor defence companies, suggests that the relationship goes beyond commercial or managerial boundaries.

The state sponsors industries such as IAI because of their desire to create the type of defence industrial base [DIB] Israel wants. The DIB parameters are determined through an in-depth assessment of Israel's strategic context, on the one hand, and the defence industry's potential contribution to reducing threats faced by Israel, on the other (Lifshitz, 2020). This is one explanation; another is that 'the innovation ecosystem Israel and its defence industries are deeply tied to violence it enacts upon a captive, subjugated native population, the Palestinians' (Abdelnour, 2023, p. 334) or a live-testing laboratory which generates field-tested arms (Feldman, The Lab, 2013). A third viewpoint considers that the DIB is shifting its focus from the military's needs to purely governments' business interests with 'the IDF growing weaker and the MoD growing stronger...' (Hania, 2016). This translates into the imbalance between what the IDF wants and what the defence industry actually produces for government's interest. Nissim Hania outlines that: 'the IDF repeatedly insists on the need for combined arms operations, while the industry continues to equip the army with innovative monolithic armaments…' (2016). In other words, industry has prevalence over the IDF's choices and needs, generating, in this way, negative implications for the military's edge and readiness.

For both cases we can conclude that the defence industry's actors supplement the state as supportive partners to help the administration pursue national and strategic objectives, albeit the respective partnerships are arranged differently according to the power relations in each country. In some cases, this puts the government's or market's interest over the needs of the military. The Italian defence industry aims to upgrade its involvement from a customer–supplier relationship to a system partnership. The example of the IFTS reveals that the defence industry plays a consultancy role in relation to the Italian government in its efforts to increase the maturity of its capabilities as an intelligent customer, at the same time promoting governments' interests through defence diplomacy tools. In the Israeli case, the government, in sponsoring the defence industry, manoeuvres industry activity pragmatically,

steering it clearly to where it serves internal, foreign, and/or economic policy. This signifies that the industry has little independence in its activities; it strictly follows the Israeli government's needs and sometimes performs functions adhering to political interests.

Table 2 sets out the KM indicators for the production and use of specialised knowledge to exploit community learning for organisational change translated into grand strategy designs. From left to right, column 1 comprises the organisational assets or capabilities (i.e., technology, culture, expertise). These organisational resources create and sustain the development of knowledge capabilities (column 2) that drive community learning and determine its efficiency or performance (column 3). Both, knowledge combination and community learning are conditioned by factors that hamper their flow (column 4) and those that promote these activities (column 5). Table 3, merges Tables 1 and 2 and utilises their indicators to outline PPPs' contribution to grand strategic designs alongside the corresponding case studies discussed below.

Table 25. 2: *Knowledge Combination and Community Learning Effectiveness*

Organisational Capability	Capability Indicators & Knowledge Combination	Efficiency of Community Learning	Inhibitors for Knowledge Combination & Learning Efficiency	Drivers for Knowledge Combination & Learning Efficiency
Technology	Technology supports and defines information sharing	Protection of collective knowledge Easy-to-access information Support to informal and formal exchange of knowledge Assessment of knowledge to combine Senior management support incl. allocation of resources Strengthening partnership culture that supports learning Building a knowledge strategy with a military and commercial focus Translation of expertise into novel ideas and action Programmed critical thinking	Failure to adopt technology	Technology that supports community learning
Structure	Partners are supported by their home structures to share and combine knowledge Innovation investments Pool of resources to choose from and select the knowledge that best fits to the partners 'goal A networked leadership Allocation of financial resources		Failure to triangulate/ and combine informal with formal knowledge Partners' divergencies Lack of company or institutional investments to support working groups and their projects	Formational/educational activities Investments Pool of resources Participatory learning
Culture	Partners come from a knowledge-sharing culture Non-linear learning and/or learning on the battlefield Trust Teamwork in combining knowledge		Reject new knowledge Lack of diversity	Shared culture Shared purpose Shared value Trust Harmonisation of expertise
Expertise	Partners understand and combine knowledge to enhance community performance to meet organisational objectives Partners work in line with their expertise Interdisciplinary knowledge is applied to formulate solutions Partners have the capability and competency in knowledge Partners organise themselves in lobbies to exert influence and change the course of action of the organisation		Lack of expertise Lack of time to learn	Project resources utilised by the partnership to learn Partners are interested to consolidate their expertise by linking previous knowledge to new information

Continues on the next page...

Information	Community members access knowledge storage in their organisation Community members create a collective knowledge storage Knowledge is constantly improved and updated	External stimuli induce knowledge sharing with regard to common resources or ad hoc tools to tackle challenges	Malformation Distortion of information	Existing database and information in the organisation are relevant to the individuals' need for efficient use Partnership database is updated constantly
Environment	Willingness to invest in innovation and R&D Ability to design a strategy		Bureaucracy Failure to adopt new knowledge	Conduct new projects Ying-yang view in combining knowledge Willingness to invest in R&D
Decision-making	Hierarchical Transactional Adhocratic Inter/ Intra-family	Transactional-collective knowledge for competitive advantages/only the fittest knowledge survives Adhocratic- collective knowledge for transformative resilience	Hierarchical-collective knowledge for predictive outputs	Participating in cross-functional teams that were responsible for key decisions, Change the frequency of decision-making Ability to robustly debate ideas

Source: *Developed by Author 2024; based upon Aujirapongpan et al.,2010 and Bontis et al.,2002*

Table 25.3: *PPP's contribution to Grand Strategic Designs*

PPP's Function and Purpose	Grand Strategic Design	PPP Case-Study	Learning Level
As system integrators: strengthen the country's institutional, military. and entrepreneurial capabilities	*Strengthening the strategic edge of a country by allowing it to adopt an active role in strategic affairs*	Cyber: Leonardo Academy (Italy) and Axon VC (Israel)	Individual Learning Level
Engineering institutional proliferations: for additional norms, rules, resources and power delegation	*Harmonise defence institutions with international expectations, strengthening institutional capacities*	Cyber: Leonardo Academy (Italy) and Axon VC (Israel)	Individual Learning Level
Anticipatory Governance: mitigate the surprise effect in decision-making	*Strengthen the organisation's capacity for purposive action to fix problems and overcome immediate impediments or obstacles without necessarily having any longer-term consideration*	Aerospace: Italy	Community Learning Level
Modelling defence innovation ecosystems: institute transformational processes that seek to improve defence resilience, sustainability, and competitiveness	*Sustainability, competitiveness, and resilience of defence ecosystem*	Aerospace: Israel	Community Learning Level

Downsides of PPP activity

Many factors negatively impact the efficiency in employing PPPs for strategic edge. These factors alter the propensity of defence organisations to learn and innovate including a lack of intellectualism in the military, strategic cultures (national vs. supranational), limited access to technology, insufficient financial resources, poor planning, bureaucracy, poor leadership, lack of trust, and the weight of regulatory barriers. While the literature recognises most of these elements, this analysis will briefly discuss trust, corruption and intellectual property rights [IPR]

In particular, the issues of trust, corruption, and IPR are all worthy of particular consideration because they illustrate the downsides of the process of engaging public-private

partnerships. Trust is necessary for ideas to be transferred. At the same time, corruption prevents innovation due to a lack of resources, as well as the issue of IPR which can impede the flow of capital and technologies to support Organisational Innovation [OI]. A lack of trust can impede the path of knowledge acquisition from giver to receiver. This is especially true when there is an imbalance between horizontal and vertical trust. In such cases where trust is seen as being compromised or lacking, it might be detrimental to knowledge sharing and therefore innovation (Hooff & Ridder, 2004). Individual institutions and sometimes even entire industries are nervous about sharing trade or product secrets. For instance, there is an ongoing battle between national defence industries and the EU Commission, according to Euroactiv (Pugnet, 2023). The focus of the debate is the Act in Support of Ammunition Production [ASAP] presented by the Commission to help the defence industry ramp up ammunition production for Ukraine (Pugnet, 2023). To ensure the timely production of the ammunition, Articles 13, 14, 15, and 18 of the Act empower the Commission to access confidential data on the industry's production capacity (EU Parliament and the Council of the EU, 2023; Pugnet, 2023). Various questions emerge here around the use of data and their security and transfer to competitors and/or other states. These concerns could discourage the production of disruptive technologies which 'provide new opportunities for the rise of EU as technological power and could be subject to corruption (Csernatoni, 2021).

Corruption, too, generally hinders any effort to organisational changes, although in some cases it can also facilitate the process. Research on corruption risks in the defence industry has been extensive, with an extensive body of knowledge and evidence now available that national actors can draw upon, providing strategic insights to the international community that inform national reform efforts. Defence sectors often lack the basic governance standards of other parts of the public sector, with oversight, transparency, and accountability requirements often overlooked (Transparency International, 2020; 2021), which also explains why Israel ranks 31st and Italy 41st out of 180 countries in the Corruption Perception Index for 2022 (Transparency International, 2022).

Resilience in both Italian and Israeli institutions is low, and procurement is characterised by secrecy and influenced by powerful defence industry actors (Transparency International, 2020). This situation does not seem to defence modernisation which nurtures the resources for grand designs, since it increases the potential for corrupt practices which in turn affect the purchase of innovative technologies and therefore, affect the military capabilities in the operational theatres, as well.

Meanwhile, IPR concerns are high on the agendas of defence establishments today – in particular with regard to information sharing between public and private partners. In a study

conducted in 2020 (McPhilips, 2020), cluster coordinators were asked to rank the importance of listed barriers to innovation on a five-point Likert scale. Respondents assigned the greatest importance to difficulties in managing joint projects and the IPR issues of participating companies (McPhilips, 2020). IPR challenges defence policymakers to strike a balance between protecting innovation and allowing accessibility to information and products. However, IPR is given limited coverage because it is not that relevant to the paper's goal of understanding how PPP's expertise influences internal transformations within the defence organisation itself. The work explains how expert knowledge promotes organisational innovation and not the negative outcomes of the process – which would require additional case studies, a team of experts, and an information clearance for the researcher considering the sensitivity of the topic for the defence sector. Further to this, as suggested in the conclusion, this work recognises the indispensability of addressing the topic of negative outcomes of OI and also its downsides in additional research and through a variety of case studies other than Italy and Israel.

Conclusions and Potential Venues of Future Work

How do defence organisations create preferred conceptualisations and employ tactics for making grand strategy utilising knowledge? For this purpose, the analysis observed the PPPs' activity in the aerospace and cyber sectors in Israel and Italy. It was intriguing to notice how countries that operate in different strategic contexts, and with no national or defence grand strategy, create concepts and employ tactics to create a grand strategy. For example, the Italian case showed that defence diplomacy proved to be efficient tools. PPPs have introduced a new strategic era in which grand strategy is the property of the partnership (Patman, 2007). In this strategic era, knowledge has become the power source to develop defence organisations that can learn.

PPPs have enacted knowledge structures enabling defence institutions and industry actors to enhance their capabilities and 'learn how to frame issues at their best advantage' (Freeman, 2021, p. 557). This makes defence grand strategy an open-ended process. It is fluid and innovative but always preserves the state-tailored offence-defence principles and is grounded in the strategic context in which the state operates and relates to the international system. This is seen in the examples from the PPP interests of Israeli Aerospace Industries [IAI], Axon Ventures, Leonardo Cyber Academy, and International Flight Training School of Leonardo. Given this, the analytical framework broke down the knowledge activities in which state and non-state actors engage into a two-level learning scale to observe how defence organisations learn to perform.

The analysis focused on the main dimensions of a grand strategy: people, resources, and interests.

There is a lot still to research on the subject of OI in defence, especially with the evolution of A.I. The topic of PPP in creating organisational change for grand strategic objectives is especially relevant when designing and consolidating the state defence strategies of tomorrow. Defence organisations will not stop innovating as they seek to ensure their competitiveness, resilience, and sustainability. New policies, actors, resources, and interests will emerge to pursue these objectives urgently, always relying on knowledge as the key tool, as this paper has shown. Therefore, future research has to do more work on how PPPs' interest in developing innovative capabilities is influenced by their ability to shape the defence organisation itself.

Acknowledgements

I wish to thank the reviewers for their useful feedback on this article. No funding was received for this project.

Data Availability Statement

The data that support the findings are available from the corresponding author (M.P) upon reasonable request.

References

Abdelnour, S. (2023). Making a Killing: Israel's Military-Innovation Ecosystem and the Globalization of Violence. *Organization Studies, 44*(2), 334-337.

Agenzia Nova. (2023). *This is what the Action Plan between Italy and Germany provides*. Retrieved January 11, 2024, from https://www.agenzianova.com/en/news/ecco-cosa-prevede-il-piano-dazione-tra-italia-e-germania/

Andonova, L. (2006). Globalization, Agency, and Institutional Innovation: The Rise of Public-Private Partnerships in Global Governance. *Colby-Working Papers in Economics*(3), 1-62.

Andonova, L. (2017). *Governance Entrepreneurs* (Kindle Edition ed.). Cambridge: Cambridge University Press.

Apostolakis, C., & Smith, L. R. (2003). Public-private partnerships, a new form of institutionalism. Katowice: Karol Akademiecki, University of Economics.

Arquilla, J., & Ronfeldt, D. (1999). *The Emergence of Noopolitik- toward an American Information Strategy.* Washington DC: RAND.

Aujirapongpan, S., Vadhanasindhu, P., Chandrachai, A., & Cooparat, P. (2010). Indicators of Knowledge Management capability for KM effectiveness. *The Journal of Information and Knowledge Management Systems , 40*(2), 183-2003.

Avant, D. D. (1993). The Institutional Sources of Military Doctrine: Hegemons in Peripheral Wars. *International Studies Quarterly, 37*(4), 409-430.

Axon VC. (2019). *About us* . Retrieved December 07, 2022, from https://www.axon.vc

Balzacq, T., Dombrowski, P., & Reich, S. (2019). *WHAT IS GRAND STRATEGY? INTERVIEW WITH THIERRY BALZACQ AND SIMON REICH*. Retrieved October 12, 2023, from

hhttps://www.sciencespo.fr/ceri/en/content/what-grand-strategy-interview-thierry-balzacq-and-simon-reich

Bandura, A. (1965). *Social foundations of thought and action: A social cognitive theory.* Englewood Cliffs: Prentice-Hall.

Barak, O., Sheniak, A., & Shapira, A. (2021). The shift to defence in Israel's hybrid military strategy. *Journal of Strategic Studies, 46*(2), 345-377.

Battaglia, M. (2022). *formiche.net-L'Italia investirà più (e meglio) in Difesa. Tutti i dettagli del documento programmatico*. Retrieved August 12, 2023, from https://formiche.net/2022/07/tempest-documento-programmatico-difesa/

Belfer Center. (2015). *Deterring Terror English Translation of the Official Strategy of the Israel Defense Forces.* Cambridge: Belfer Center.

Ben-Horin, Y., & Posen, B. (1981, September). *RAND-Israel's Strategic Doctrine.* Retrieved April 30, 2024, from https://www.rand.org/content/dam/rand/pubs/reports/2007/R2845.pdf

Bennet, A., & Bennet, D. (2004). The Partnership Between Organizational Learning and Knowledge Management. In C. W. Holsapple (Ed.), *Handbook on Knowledge Management 1. International Handbooks on Information Systems,* (pp. 439-456). Berlin: Springer.

Biscop, S. (2021). *Grand Strategy in 10 Words- A Guide to Great Power Politics in the 21st Century* (1st - Kindle Oasis 10a ed.). Bristol: Bristol University Press.

Bontis, N., Crossan, M., & Hulland, J. (2002). Managing an Organizational Learning System by Aligning Stocks and Flows. *Journal of Management Studies, 39*(4), 432-469.

Bourdieu, P. (1990). *TheLogic of Practice* (1st ed.). Cambridge: Polity Press.

Brands, H. (2012, August). *The Promise and Pitfalls of Grand Strategy.* Retrieved August 2023, from US Army War College: http://www.jstor.com/stable/resrep11597

Braw, E. (2022). *Italy Is a Quiet Pillar of NATO's Aerial Policing*. Retrieved January 11, 2024, from https://www.defenseone.com/ideas/2022/02/italy-quiet-pillar-natos-aerial-policing/362230/

Buchanan, R. (2008). Introduction: Design and Organizational Change. *Design Issues, 24*(1), 2-9.

Butz, M. V., & Pezzulo, G. (2011). Anticipatory learning . In *Encyclopedia of the Sciences of Learning* (pp. 263-266). Dordrecht: Springer.

Carayannis, E. G., Pirzadeh, A., & Popescu, D. (2012). *Institutional Learning and Knowledge Transfer Across Epistemic Communities* (1st ed.). London: Springer.

Castaneda, D. I., & Rios, M. F. (2007). From Individual Learning to Organizational Learning. *Electronic Journal of Knowledge Management, 5*(4), 363-372.

Castro, V., & Janssens, J. G. (2011, June). *Mixed Private-Public Ownership Companies "Empresa Mixta".* Retrieved April 27, 2024, from https://ppp.worldbank.org/public-private-partnership/sites/ppp.worldbank.org/files/documents/EmpresaMixtaAFDpublicationJune7_0.pdf

Cavelty, M. D., & Sute, M. (2009). Public-Private Partnerships are no silver bullet. An expanded governance model for critical infrastructure protection. *International Journal of Critical Infrastructure Protection, 4*(2), 179-187.

Cohen, R. (2016). Consciousness campaigns in the new era. *Israel Defence*(32), 58-60.

Coticchia, F., & Celso, M. M. (2024). Still on the same path? Italian foreign and defence policy in the Enlarged Mediterranean. *Mediterranean Politics, https://doi.org/10.1080/13629395.2023.2294252*.

Cottey, A., & Forster, A. (2004). Strategic engagement: defence diplomacy as a means of conflict prevention. *The Adelphi Papers, 44*(365), 15-30.

Crossan, M. M., Lane, H. W., & White, R. E. (1999). An Organizational Learning Framework: From Intuition to Institution. *The Academy of Management Review, 24*(3), 522-537.

Department of Economic & Social Affairs- UN. (2016). Public-Private Partnerships and the 2030 Agenda for Sustainable Development: Fit for purpose? Department of Economic & Social Affairs.

DiMaggio, P. .., & Walter Powell. (1983). The iron cage revisited" institutional isomorphism and collective rationality in organizational fields. *American Sociological Review, 48*, 147-160.

Drab, L. (2018). Defence diplomacy – an important tool for the implementation of foreign policy and security of the state. *Security & Defence Quarterly, 20*(3), 57-71; https://doi.org/10.5604/01.3001.0012.5152.

Drinkuth, A., H.Riegler, C., & Wolff, R. (2001). Labour Unions as Learning Organizations and Facilitators. In A. B. Meinolf Dierkes, & I. Nonaka (Eds.), *Handbook of Organizational Learning and Knowledge* (pp. 446-461). Oxford: Oxford University Press.

EEAS. (2023). *PeSCo Factsheet.* Retrieved April 8, 2023, from https://www.consilium.europa.eu/media/53013/20211115-pesco-projects-with-description.pdf

EESC. (2012). Security industrial policy – Action plan for an innovative and competitive security industry-COM(2012) 417 final. Brussles.

Eisenkot, G., & Siboni, G. (2019). *Guidelines for Israel's National Security Strategy* (1st ed.). Washington: THE WASHINGTON INSTITUTE FOR NEAR EAST POLICY.

EU Parliament and the Council of the EU. (2023). Regulation (EU) 2023/1525 of the European Parliament and of the Council of 20 July 2023 on supporting ammunition production (ASAP). *Official Journal of the European Union L 185/7*, 7-25.

Evron, Y., & A.Bitzinger, R. (2023). *The Fourth Industrial Revolution and Military Civil Fusion- A New Paradigm for Military Innovation?* (Yoram Evron; Richard A.Bitzinger ed.). Cambridge: Cambridge University Press.

Feldman, Y. (Director). (2013). *The Lab* [Motion Picture]. Israel.

Foucault, M. (1970). *The Order of Things.* New York: Random Hourse.

Freeman, L. (2021). Grand Strategy - The History of a Concept. In T. B. R.Krebs (Ed.), *The Oxford Handbook of Grand Strategy* (pp. 25-41). Oxford: OUP Oxford.

Gaddis, J. L. (2018). *What is Grand Strategy?' American Grand Strategy After War* (1st KIndle Oasis 10a ed.). London: Penguin.

Garsten, C. & Nyqvist, A. (2013). Entries: engaging organisational worlds. In: C. Garsten & A. Nyqvist, (Eds.), *Organisational Anthropology: Doing ethnography in and among complex organisations (Anthropology, Culture and Society)* (pp 15-58.). London: PlutoPress, pp. Kindle edition

Greve, C., & Hodge, G. (2016). *Rethinking Public-Private Partnerships, Strategies for turbulent times* (2nd ed.). Abingdon: Routledge.

Haas, P. (1990). Do Regimes Matter? Epistemic Communities and Mediterrenean Pollution Control. *International Organizations, 43*(3), 377-403.

Hall, D. (2008). PPPs in the EU - a critical appraisal. St. Petersburg: ASPE Conference. Retrieved from https://gala.gre.ac.uk/id/eprint/2880/1/2008-11-PPPs-crit.pdf

Ham, H. V., & Koppenjan, J. (2001). Building public-private partnerships: Assessing and managing risks in port development. *Public Management Review , 3*(4), 593-616.

Hania, N. (2016). *IDF- Dado Center -Transformations in the Israeli Defense Development and Production System, and the Contemporary Relevance*. Retrieved August 21, 2023, from https://www.idf.il/en/mini-sites/dado-center/vol-6-force-design-a/transformations-in-the-israeli-defense-development-and-production-system-and-the-contemporary-relevance/

Haque, S. M. (2004). Governance based on partnership with NGOs: implications for development and empowerment in rural Bangladesh. *International Review of Administrative Sciences , 2*(2), 271-290.

Hasik, J. (2016). Defense Entrepreneurship How to Build Institutions for Innovation Inside the Military. *Joint Force Quarterly, 81*(2nd Quarter), 112-117.

Heidenkamp, H., Louth, J., & Taylor, T. (2013). The State–Defence Industrial Relationship: Government as Sponsor. *Whitehall Papers, 81*(1), 61-97.

Hill, A. (2015). The US Army War College Quarterly: Parameters The US Army War College Quarterly: Parameters. *Parameters, 45*(1), 85-98.

Hodge, G., & Greve, C. (2005). *The Challenge of Public–Private Partnerships-Learning from International Experience* (1st ed.). Cheltenham: Edward Elgar.

Hooff, B. v., & Ridder, J. A. (2004). Knowledge sharing in context: the organizatonal commitment, communication climate and CMC use on knowledge sharing. *Journal of Knowledge Management, 8*(6), 117-130.

Howard, M. (2001). Grand Strategy in the Twentieth Century. *Defence Studies, 1*(1), 1-10.

Huff, A. S. (1990). Mapping Strategic Thought. In *Mapping strategic thought* (pp. 11-49). Chichester: Wiley.

Interview between the Author and Rear Adm (Rtd)Ophir Shoham, Axon VC (2021)

IAI. (nd). *iai.co.il-history-IAI and the Security of Israel*. Retrieved July 23, 2023, from https://www.iai.co.il/about/history

Jones, C. (2022). Introduction. In C. J. Petersen (Ed.), *Grand Strategy in the Contemporary Middle East: The Concepts and Debates* (pp. 1-15). Berlin: Gerlach Press.

Kanon, S. (2008). *From fighter pilot to entrepreneur*. Retrieved July 29, 2021, from https://www.israel21c.org/from-fighter-pilot-to-entrepreneur/

Kapilashrami, A. (2010). *Understanding Public Private Partnerships: The Discourse, The Practice, And The System Wide Effects Of The Global Fund To Fight Aids, Tuberculosis, And Malaria (eThesis).* Retrieved March 29, 2020, from http://etheses.qmu.ac.uk/369/

Kappeler, A., & Nemoz, M. (2010). *Public-Private Partnerships In Europe – Before And During The Recent Financial Crisis.* Brussels: European Investment Bank.

Ken, S. (2003). Achieving organizational learning across projects. North America, Baltimore, MD: Paper presented at PMI® Global Congress 2003.

Kennedy, P. (1991). *Grand Strategies in War and Peace* (1st ed.). New Haven: Yale University Press.

Klein, S. B., Robertson, T. E., & Delton, A. W. (2010). Facing the future: Memory as an evolved system for planning future acts . *Mem Cognitive, 38*(1), 13-22.

Kucharska, W., & Erickson, G. S. (2023). Tacit knowledge acquisition & sharing, and its influence on innovations: A Polish/US cross-country study. *International Journal of Information Management, 71*, 1-24.

Layton, P. (2018). *Grand Startegy (E-book, Kindle Oasis 10a).*

Leonardo. (2022a). *Cyber Academy*. Retrieved December 5, 2022, from https://cyberacademy.leonardo.com/en/home

Leonardo. (2022b). *Leonardo's commitment to disseminating cyber expertise*. Retrieved December 6, 2022, from https://www.leonardo.com/en/news-and-stories-detail/-/detail/leonardo-cyber-expertise-diffusion

Leonardo. (nd). *The International Flight Training School (IFTS)*. Retrieved from https://aircraft.leonardo.com/en/customer-support/international-flight-training-school

Lifshitz, Y. (2020). *The Strategic Importance of the Defense Industries in Israel.* Retrieved November 18, 2023, from https://www.inss.org.il/wp-content/uploads/2020/08/Memo202_e-23-33.pdf

Littoz-Monnet, A. (2017). *The Politics of Expertise in International Organizations* (1st ed.). London: Routledge.

Luttwak, E. (2001). *Startegy- The Logic of War and Peace* (1st ed.). Cambridge MA: The Belknap Press of Harvard University Press.

Madeddu, D. (2022). *ilsole24ore-Piloti di caccia, investiti nella formazione 200 milioni nella base di Decimomannu*. Retrieved May 23, 2023, from https://www.ilsole24ore.com/art/piloti-caccia-investiti-formazione-200-milioni-base-decimomannu-AExOljGC?refresh_ce=1

McPhilips, M. (2020). Trouble in Paradise? Barriers to Open Innovation in Regional Clusters in the Era of the 4th Industrial Revolution. *Journal of Open Innovation: Technology, Market, and Complexity, 6*(3), 1-14.

Merindol, V., & Versailles, D. W. (2020, July). The (R)evolution of Defence Innovation Models: Rationales and Consequences. *IRIS Nr.60*, pp. 1-27.

Ministero della Difesa. (2021a). *Approvato il Documento Programmatico Pluriennale 2021-2023*. Retrieved February 19, 2023, from https://www.difesa.it/Primo_Piano/Pagine/Documento-Programmatico-Pluriennale.aspx

Ministero della Difesa. (2021b). *Difesa.it-Documento Programmatico Pluriennale della Difesa per il Triennio2021-2023.* Retrieved August 17, 2023, from https://www.difesa.it/Content/Documents/20210804%20DPP%202021-2023%20per%20pubblicazione.pdf

Ministero della Difesa. (2021c). *Difesa.it-Defence Industrial Policy Directive.* Retrieved October 12, 2023, from https://www.difesa.it/EN/Minister_of_Defence/Documents/DPI_2022_Versione_Inglese.pdf

Ministero della Difesa. (2022a). DOCUMENTO PROGRAMMATICO PLURIENNALE DELLA DIFESA PER IL TRIENNIO 2022-2024. Rome: Ministero della Difesa.

Ministero della Difesa. (2022b). National Military Policy Directive. Rome: Ministero della Difesa.

Ministero della Difesa. (2022c). *The Chief of Defence Strategic Concept September.* Rome: Ministero della Difesa.

Ministero della Difesa. (2022d). Defence and Security Strategy for the Mediterranean - 2022. Rome: Ministero della Difesa.

NATO Science & Technology Organization. (2019). *Public Private Partnership in a NATO Context.* Brussels: NATO.

OECD. (2012, May). *OECD Principles for Public Governance of Public-Private Partnerships.* Retrieved May 14, 2024, from https://www.oecd.org/gov/budgeting/oecd-principles-for-public-governance-of-public-private-partnerships.htm

OECD. (2024). *Recommendation of the Council on OECD Legal Instruments Guidelines on Corporate Governance of State-Owned Enterprises.* Paris: OECD.

Olio, L. d. (2022). *Leonardo, l'accademia dei talenti della cybersecurity dal cuore hi-tech*. Retrieved December 6, 2022, from https://www.repubblica.it/dossier/economia/valore-italia/2022/09/19/news/leonardo_laccademia_dei_talenti_della_cybersecurity_dal_cuore_hitech-366381455/

Ortal, E. (2024). *Israel's First Total War And Its Ramifications*. Retrieved April 30, 2024, from https://www.hoover.org/research/israels-first-total-war-and-its-ramifications#_ftnref1

Patman, R. G. (2007). *Globalization and Conflict National Security in a 'New' Strategic Era* (1st ed.). London: Routledge.

Posen, B. (1984). *The Sources of Military Doctrine: France, Britain, and Germany between the World Wars. Balzacq, Thierry; Krebs, Ronald R.. The Oxford Handbook of Grand Strategy (Oxford Handbooks) (p. 20). OUP Oxford. Kindle Edition.* (1st ed.). Ithaca: Cornell University Press.

Pugnet, A. (2023). *Euractiv -Defence industry nervous about sharing trade secrets with EU*. Retrieved September 9, 2023, from https://www.euractiv.com/section/defence-and-security/news/defence-industry-nervous-about-sharing-trade-secrets-with-eu/

RAND Corporation. (1999). *Use of PPPs to Meet Army Needs* (1st ed.). Santa Monica: Arroyo Centre; RAND.

Roberts, N. C., & King, P. J. (1991). Policy Entrepreneurs: Their Activity Structure and Function in the Policy Process. *Journal of Public Administration Research and Theory, 1*(2), 147-175.

Rodman, D. (2005). *Defense and Diplomacy in Israel's National Security Experience* (1st ed.). Brighton: Sussex Academic Press.

Ronfeldt, D., & Arquilla, J. (2021, January 30). *Rethinking Strategy and Statecraft for the Information Age: Rise of the Noosphere and Noopolitik- SSRN papers.* Retrieved November 2, 2023, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3910628

Ruggie, J. G. (1975). International Responses to Technology: Concepts and Trends. *International Organizations, 29*(3), 557-583.

Sánchez-Carreira, M. d., Vence, X., & Rodil-Marzábal, Ó. (2020). The Role of State-Owned Enterprises as Drivers of Innovation. In X. V.-M. María del Carmen Sánchez-Carreira (Ed.), *The Routledge Handbook of State-Owned Enterprises* (pp. 619-637). London: Routledge.

Sedjari, A. (2004). Public-private partnerships as a tool for modernising public administration. *International Review of Adnministrative Sciences, 70*(2), 291-306.

Shamir, E. (2019). Israel. In T. Balzacq, P. Dombrowski, & S. Reich (Eds.), *Comparative Grand Strategy A Framework and Cases* (pp. 217-239). Oxford: Oxford University Press.

Sheffer, G., & Barak, O. (2013). *Israel's security networks- a theoretical and comparative sector* (1st Edition- Kindle version ed.). Cambridge: Cambridge University Press.

Silove, N. (2018). Beyond the Buzzword: The Three Meanings of "Grand Strategy". *Security Studies, 27*(1), 27-57; https://doi.org/10.1080/09636412.2017.1360073.

Technion Haifa. (2017). *GRAND STRATEGY FOR ISRAEL: Reflections and Directions.* Haifa: The Samuel Neaman Institute of National Policy Research.

The Peninsula Qatar. (2023). Retrieved January 11, 2024, from https://thepeninsulaqatar.com/editorial/12/09/2023/consolidating-qatar-italy-ties

Tierney, D. (2021). The Future of Sino-U.S. Proxy War. *Texas National Security Review, 4*(2), 49-73; http://dx.doi.org/10.26153/tsw/13198.

Transparency International. (2020). *Government Defence Industry Index 2020*. Retrieved December 23, 2023, from https://ti-defence.org/gdi/

Transparency International. (2021). *Transparency International – Analysing Defence Industry Influence on the Italian Policy Agenda.* London: Transparency International.

Transparency International. (2022). *Corruption Perception Index*. Retrieved December 23, 2023, from https://www.transparency.org/en/cpi/2022

Turner, J. R., & Baker, R. M. (2019). Complexity Theory: An Overview with Potential Applications for the Social Sciences. *Systems, 7*(1), 1-22.

UNECE. (2012). UNECE International Conference "Taking Public-Private Partnerships forward: New Opportunities for Infrastructure Development in Transition Economies" (21-22 October 2008), jointly organized by the State corporation "Bank for Development and Capacity-build. UNECE.

Wojewnik-Filipkowska, A., & Wegrzyn, J. (2019). Understanding of Public–Private Partnership Stakeholders as a Condition of Sustainable Development. *Sustainability, 19*(11), 1-16.

Zweibelson, B. (2022). *Understanding Emergence: How Complexity Theory Requires Getting Out of the Military's Favored Newtonian Box*. Retrieved December 30, 2023, from https://benzweibelson.medium.com/understanding-emergence-how-complexity-theory-requires-getting-out-of-the-militarys-favored-bf914e06f1e

Zweibelson, B. (2023). *Understanding the Military Design Movement- War, Change and Innovation - Routledge Studies in Conflict, Security and Technology* (1st- Kindle Oasis 10a ed.). London: Routledge.