Technical Evaluation Report (TER) HFM-361

Research Symposium (RSY)

Mitigating and Responding to Cognitive Warfare

Madrid, Spain

13 and 14 November 2023

P.M.H. Buvarp
Instituttveien 20,
2007, Kjeller
NORWAY

paul-magnus-hjertvik.buvarp@ffi.no

ABSTRACT

This Technical Evaluation Report for the HFM-361 Symposium, "Mitigating and Responding to Cognitive Warfare," held in Madrid, Spain, in November 2023, presents a comprehensive overview of the event's proceedings, insights, and conclusions. This symposium brought together a diverse group of international experts, practitioners, and academics from various disciplines to address the multifaceted challenges of cognitive warfare. The report captures the essence of the symposium, encompassing the breadth of topics discussed, which ranged from the theoretical underpinnings of cognitive warfare to practical applications in military and civilian contexts. Papers and presentations were given within five categories: Keynotes, Understanding and Conceptualizing Cognitive Warfare, Strategies and Models for Cognitive Warfare, Technological and Societal Aspects of Cognitive Warfare, and Cognitive Warfare in the Field and in Practice. The report highlights the symposium's success in fostering interdisciplinary dialogue, which was instrumental in enhancing mutual understanding among experts from different fields. This gathering underscored the dynamic nature of cognitive warfare, emphasizing the need for adaptable and comprehensive strategies to address evolving threats. Overall, the HFM-361 Symposium contributed significantly to the NATO scientific community's understanding of cognitive warfare, marking important steps towards the maturity of this field within the alliance. The insights and collaborative spirit fostered by this symposium are invaluable in developing effective strategies to counter the complex challenges posed by cognitive warfare.

Keywords: *Cognitive Warfare; Human Factors; Information Warfare; Psychological Operations.*

1.0 INTRODUCTION

In an era marked by escalating global tensions and the rapid evolution of technology, the HFM-361 symposium, held on 13-14 November in Madrid, Spain, was geared to address the multifaceted challenges of cognitive warfare. This symposium, following the workshop conducted in Norway in 2022, brought together a diverse group of experts, practitioners, and academics.

In total, 129 people attended the Symposium, representing 24 nationalities, as well as NATO Allied ACT and HQ. Also in attendance was the NATO Chief Scientist, Dr. Bryan Wells, and the NATO Science & Technology Organization's (STO) Collaboration Support Office (CSO) Director John-Mikal Størdal. Their collective aim was to explore synergies and common challenges in the complex nature of cognitive warfare, a field increasingly recognized for its potentially game-changing impact on future military operations.

With work already underway within numerous Exploratory Teams (ETs) and Research Task Groups (RTGs) as well as independent work conducted by individual research institutions, there was much to discuss. This collaborative effort was in line with the NATO Science & Technology Board's (STB) March 2022 initiative, which identified cognitive warfare as a primary challenge within the STO Collaborative Programme of Work (CPoW). The aim was to foster research that could strengthen NATO's defence against the multifaceted nature of cognitive warfare, requiring expertise across borders both national and scholarly.

The symposium responded to a world increasingly confronted by cyber, hybrid, and other asymmetric threats, including sophisticated disinformation campaigns as emphasized in the NATO Summit declarations of 2021 and 2022. These summits highlighted the urgent need for NATO to develop strategies to counteract the operations of state and non-state actors, including Russia and China, in the realm of cognitive warfare.

Cognitive warfare, a domain that blends military strategy with a broad spectrum of academic fields including neuroscience, psychology, information technology, and more, poses both challenges and opportunities. It necessitates bridging diverse terminologies and methodologies while offering a rich foundation for effective counter strategies. Indeed, cognitive warfare is not confined to military perspectives alone; it spans political and social environments, leveraging technological advancements and novel tactics to manipulate cognition and behaviour. Its focus on altering cognitive processes and actions, boosted by digital ecosystems, artificial intelligence (AI), and the Internet of Things (IoT), underscores its expansive nature. The HFM-361 Symposium intended to address these aspects, aiming to strengthen collective understanding and response capabilities against cognitive threats.

The HFM-361 Symposium is just one approach aimed to enhance NATO's collective capacity to sense, make sense of, and counteract cognitive warfare, and to develop legal and ethical procedures to address the novel field. The outcomes and discussions from this symposium are set to inform future research activities, investments, and strategies, further strengthening NATO's preparedness and response in the realm of cognitive Warfare.

1.1 Theme

The theme of the symposium, "Mitigating and Responding to Cognitive Warfare," was carefully chosen to reflect the growing importance of the cognitive dimension in modern warfare. In an era where hybrid methods combine traditional warfare tactics with advanced technologies and innovative delivery techniques, understanding and countering cognitive threats has become a significant aspect of conflict. These methods, including propaganda, deception, and disinformation, target both military and civilian domains, necessitating a strong collaboration between defence and security sectors.

1.2 Purpose and Scope

The symposium's purpose was to delve into the multi-domain battlefield of cognitive warfare, exploring how behaviour can be influenced by protecting or manipulating cognition to gain strategic advantage. The discussions aimed to enhance the common understanding of ways to mitigate and respond to sophisticated cognitive warfare tactics and procedures.

Cognitive superiority, defined as the ability to outthink and outmanoeuvre adversaries through advanced situational awareness, data management, and cognitive processes, is identified as a key advantage. The symposium emphasized the need for NATO to develop and maintain a comprehensive approach to achieving and sustaining cognitive superiority, especially in light of the potential threats posed by state and non-state actors, as recognized in the NATO Summits of 2021 and 2022.

The scope of the symposium extended to examining cognitive warfare from a wide array of academic fields and traditions. The event sought to address the urgent need for NATO to obtain the capabilities to effectively resist, mitigate, and counter such warfare on its member countries and develop effective norms around its use.

Building on prior NATO initiatives and studies, the HFM-361 Symposium intended to consolidate existing knowledge, propose future research paths, and develop strategies for education and training in the realm of cognitive warfare. The symposium was designed not just to share insights and experiences but also to foster a collaborative environment for developing comprehensive responses to the cognitive challenges facing NATO and its allies today.

2.0 EVALUATION

In sum, the broadness of the subject ensured a wide variety of approaches in the presentations of the symposium. This presents certain challenges to synthesising a totality as an evaluation of the scientific position the allies find themselves in. Therefore, synthesis is in this report constrained to a handful of categories which together demonstrate the fullness of the symposium.[1] Five such categories have been identified: i) Keynotes; ii) Understanding and Conceptualizing Cognitive Warfare; iii) Technological and Societal Aspects of Cognitive Warfare; iv) Strategies and Models for Cognitive Warfare; and v) Cognitive Warfare in the Field and in Practice. A discussion of the challenges and merits of such a broad area of impact is undertaken in part 3, Conclusions.

2.1 Keynotes

The keynote speeches were meant to set the stage for the symposium. One of the keynote speeches was delivered also as a paper, whereas the other two were presentations.

Ignacio Nieto's[2] paper, "Spanish Approach to Cognitive Warfare," discusses the evolving role and significance of cognitive warfare on the international stage, with a particular focus on the Spanish Armed Forces. The paper highlights cognitive warfare as a strategic alternative to force or diplomacy, targeting the three pillars of Clausewitz's trinity—people, armed forces, and government—through information manipulation. Nieto emphasizes the blurred lines between peace and war in the current era, complicating the development of responses and the identification of victory and defeat. He underscores the importance of understanding operational art in the cognitive domain, where interconnected capabilities are crucial for planning and executing operations. The paper also reflects on the substantial impact of technological advancements, particularly in neuroscience, in reshaping warfare and narrowing the military power gap. Nieto's work provides a detailed view of the Spanish approach to cognitive warfare, highlighting the need for continuous innovation within the Armed Forces to effectively navigate this complex domain.

Janis Berzins'[3] presentation, "Cognitive Battleground: Understanding the Russian Perspective," delved into the Western and Russian viewpoints on cognitive warfare. Berzins traced the evolution of the Western definition of cognitive warfare from the hyperconnectivity of the 2000s, emphasizing the role of algorithms and technology. The presentation highlighted Russia's belief that the West is waging a civilizational war intended to Westernize Russia. A key concept discussed was 'reflexive control,' a tactic aimed at influencing an adversary's decision-making process by shaping their perception of information. It was argued that this aligns with Russian intelligence efforts to understand and manipulate the decision-making processes of adversaries. Berzins referenced Russian theorists like Andrey Ilnitsky and Karavaev, offering insights into

[1] The symposium consisted nearly exclusively of presentations of submitted academic papers. It is these papers that form the backbone of this evaluation. Nevertheless, the presentations themselves, and certainly the discussions surrounding them also inform this report.

[2] Ignacio Nieto, Head of Strategic Conduct of Operations of the Joint Staff, Spain.

[3] Janis Bezins, Director, Center for Security and Strategic Research (CSSR) at the National Defense Academy, Latvia.

Russia's approach to cognitive warfare. The presentation underscored that Russia views cognitive warfare as a form of mental warfare against the West, adding depth to the understanding of the differing perspectives and strategies in the realm of cognitive conflict.

Jean-Marc Rickli's[4] presentation, "Subversion in the 21st Century: Emerging Technologies and Cognitive Warfare," explored the evolving context of warfare in the modern era, emphasizing the impact of globalization, privatization, securitization, and mediatisation. He introduced the concept of surrogate warfare, where states externalize strategic and operational aspects of war, often through technology, which itself acts as a surrogate in conflicts. Central to Rickli's argument is the idea of cognitive warfare as a form of subversion, particularly in the context of emerging technologies. Rickli posited that significant technological advancements are reshaping the frontier of cognitive warfare, suggesting that subversion, powered by these advancements, will increasingly supersede traditional forms of coercion. This perspective presents cognitive warfare as a key mode of conflict in the 21st century, driven by technological innovations that challenge conventional understandings.

2.1.1 Notes from Discussions

The keynote panel discussion highlighted key strategies and challenges in preparing for and countering cognitive threats. The importance of red-team training and wargaming was emphasized as essential tools for understanding and simulating subversion tactics. However, concerns were raised about their limitations due to cultural biases. Panelists stressed the need to adopt the mindset of both state and non-state adversaries to effectively train forces and societies in responding to cognitive warfare. The discussion also acknowledged the changing nature of warfare, noting the cognitive domain's unique challenges to traditional military structures and the need for a broader societal and governmental response.

Technological advancements and their implications in cognitive warfare formed a significant part of the conversation. The rapid pace of development in technology, especially in the commercial sector, was noted as a crucial factor influencing the dynamics of cognitive warfare. The role of big companies and the commercial sector in driving technological innovation, in contrast to the relatively smaller scale of the defense sector, was discussed. This aspect brought to light the moral and ethical considerations in the domain of cognitive warfare, particularly regarding freedom of expression and the necessity for comprehensive debates and regulations in this evolving field.

Questions from the audience prompted discussions on identifying and understanding idiosyncratic fragilities within nations, the proactive versus reactive roles of NATO in cognitive warfare, and strategic advice for heads of states. The panelists underscored the importance of social research in understanding national characteristics, the need for NATO to adopt a more proactive and anticipatory stance, and the value of investing in foresight and collaborative efforts among NATO nations. The discussion concluded with a consensus on the complexity of cognitive warfare and the necessity for a multifaceted approach to build resilience against these emerging threats.

2.2 Understanding and Conceptualizing Cognitive Warfare

These broader papers and presentations collectively offer a comprehensive framework for cognitive warfare, integrating perspectives from social science, military strategy, psychology, neuroscience, and technology. They can be viewed as the more foundational papers, seeking to understand or conceptualize the phenomenon in different ways.

Rebecca Goolsby's[5] "Social Science and Cognitive Security" critically examines the evolution of disinformation and propaganda in the digital age, focusing on their impact on social organization and group

[4] Jean-Marc Rickli, Head of Global and Emerging Risks at the Geneva Centre for Security Policy, Switzerland.

[5] Rebecca Goolsby, Office of Naval Research, USA.

identities. Goolsby emphasizes the significance of social sciences in understanding and mitigating these threats, particularly in the realm of cognitive warfare. The paper explores how social cyber-attacks, leveraging cognitive biases and socialization processes, manipulate public opinion and identity through social media. It underscores the necessity of cognitive security, advocating for more research in cognitive linguistics, social identity, and narrative construction to defend against psychological operations and information manipulation. This work highlights the intersection of cognitive processes with security challenges, showcasing the vital role of social sciences in combating cognitive warfare in today's interconnected world.

The paper "Value Differences: A Starting Point for Influence" by Bruce Forrester[6] and collaborators examines the impact of value systems on cognitive warfare, focusing on the narrative and behavioural differences between democratic and autocratic societies. Using the Schwartz model, the authors analyse values in various contexts, including democratic countries and far-right extremism in France, to understand their influence in the information environment. This research highlights the strategic importance of recognizing and leveraging value differences in military operations. It aligns with Goolsby's work on the broader role of social sciences in cognitive security, specifically demonstrating how values, as a key aspect of social science, can be utilized in cognitive operations and information warfare.

"The understanding of Cognitive Warfare in comparative perspective: Taking stock and bridging the gap to extant literatures", a paper by Christoph Deppe, Alexandru Fotescu, and Gary Schaal[7] presents a comprehensive analysis of the cognitive Warfare concept, emphasizing its evolving nature within both military and academic discourses. It explores the concept of cognitive Warfare in relation to neighbouring concepts like Hybrid Threats and Foreign Information Manipulation and Interference (FIMI), highlighting the challenges in defining and operationalizing these concepts due to their continuous evolution and varying interpretations across different institutional spheres. The paper underscores the importance of mutual intelligibility between military and academic research for effective communication and constructive research in this field. This paper complements Goolsby's and Forrester's works by adding a detailed perspective on the institutional and conceptual complexities of cognitive Warfare.

The paper "The UnCODE System: A Neurocentric Systems Approach for Classifying the Goals and Methods of Cognitive Warfare" by Torvald F. Ask[8] and colleagues introduces the UnCODE system, a comprehensive framework for understanding and categorizing cognitive warfare tactics. This system is neurocentric, conceptualizing cognitive warfare goals from a perspective of how adversarial methods interact with neural information processing. It identifies five main classes of goals—Unplug, Corrupt, disOrganize, Diagnose, and Enhance—and categorizes methods based on direct or indirect access to the target's neural system. This innovative approach emphasizes the importance of a unified, domain- and species-agnostic framework for understanding cognitive warfare, bridging the gap between human and nonhuman cognition.

[6] Bruce Forrester, Defence Research and Development Canada, Canada; Valentina Dragos, ONERA French Aerospace Lab, France; Marco Marsili, Research Centre of the Institute for Political Studies of Univesidade Catolica Portuguesa and Department of Philosophy and Cultural Heritage of Ca Forscari University of Venice, Portugal and Italy; and Magnus Rosell, Swedish Defence Research Agency, Sweden.

[7] Christoph Deppe, Alexandru Fotescu, and Prof. Dr. Gary S. Schaal, Helmut-Schmidt-University/University of the Federal Armed Forces Hamburg, Germany.

[8] Torvald F. Ask, Department of Information Security and Communication Technology at the Norwegian University of Science and Technology and the Faculty of Health, Welfare and Organization at Østfold University College, Norway; Ricardo G. Lugo, Maritime Academy at the Tallinn University of Technology and the Centre for Digital Forensics and Cyber Security at the Tallinn University of Technology, Estonia; Stefan Sütterlin, Faculty of Health, Welfare and Organization at the Østfold University College, Norway, the Centre for Digital Forensics and Cyber Security at the Tallinn University of Technology, Estonia, and the Faculty of Computer Science at the Albstadt-Sigmaringen University, Germany; Matthew Canham, Beyond Layer Seven, USA; Daniel Hermansen, Cyber Defense at the Norwegian Armed Forces, Norway; and Benjamin J. Knox, Department of Information Security and Communication Technology at the Norwegian University of Science and Technology, the Faculty of Health, Welfare and Organization at the Østfold University College, and Cyber Defense of the Norwegian Armed Forces, Norway.

It underlines the necessity of interdisciplinary approaches, integrating insights from neuroscience to develop effective cognitive Warfare strategies, thus adding to the perspectives of Goolsby and Forrester.

Frank Flemisch's[9] "Human-Machine Teaming Towards a Holistic Understanding of Cognitive Warfare" focuses on the integration of human cognition and machine intelligence in the context of cognitive warfare. Flemisch illustrates how human-machine teaming has evolved and its implications for cognitive warfare. He emphasizes the necessity of a holistic approach that considers not just individual cognitive processes, but also the interactions between humans, machines, and larger systems. This approach aims to enhance situational awareness and decision-making in complex and uncertain environments typical of modern warfare. The paper extends the arguments from the previous papers to show the metaphorical bridge between social, neurological and technical considerations required to understand cognitive warfare.

The synthesis of these perspectives presents a layered understanding of cognitive warfare. The integration of socio-cultural, strategic military, neural, and technological insights provides a holistic view of the cognitive domain in modern warfare. This underscores the need for an interdisciplinary approach in countering cognitive threats.

2.2.1 Notes from Discussions

The extensive attributes of cognitive warfare were explored, emphasizing the need for coordination in research and the utility of frameworks like UnCODE for organizing and interpreting fieldwork data. Additionally, the conversation touched on the importance of narratives and sensemaking, particularly how history and previous experiences shape cognitive responses in warfare. General discussions also delved into various disciplines' definitions of narratives, highlighting the challenges of overcoming conceptual differences and considering the cognitive capabilities training framework.

2.3 Technological and Societal Aspects of Cognitive Warfare

Robin Burda's[10] paper "Cognitive Warfare – Problem for the Brain, Opportunity for the Machine" offers a comprehensive analysis of cognitive warfare's evolution and impact in the digital era, emphasizing the critical role of technology in shaping modern warfare strategies. Burda delineates the transition from traditional propaganda to sophisticated cognitive warfare tactics, highlighting the pivotal role of advancements in communication technologies, particularly the internet and social media. These platforms have transformed information dissemination, enabling a more participatory form of propaganda and amplifying the reach and complexity of information warfare. Burda argues for the essential integration of artificial intelligence (AI) and machine learning (ML) in defence against cognitive warfare, given the sheer volume and pace of information flow. The paper concludes that while cognitive warfare poses a formidable challenge to democratic societies, leveraging the same technologies for defence purposes and adopting a whole-of-society approach are crucial for minimizing its impact and safeguarding democratic values.

The paper "Framework for Cognitive Warfare Situational Awareness Visualization" by Mario Aragonés, Alfonso Climente, Israel Pérez and Manuel Esteve[11] delves into the intricate role of cognitive processes in modern warfare, presenting a comprehensive framework for understanding and visualizing cognitive warfare's dynamics. It defines situational awareness (SA) as the perception of environmental elements within a defined volume of time and space, crucial for decision-making in warfare. This paper expands the concept of SA beyond traditional domains, incorporating psycho-social components like cultural elements, human behaviour, and the impact of social networks and media. The authors propose an integrative

[9] Frank Flemisch, Human Systems Integration at RWYTH Aachen University, Germany,

[10] Robin Burda, Department of Political Science at Masaryk University, Czechia.

[11] Mario Aragonés, MSc., Alfonso Climente, Ph.D., Israel Pérez, Ph.D., and Manuel Esteve, Full Professor, Distributed Real Time Systems Lab at Universitat Politécnica de Valéncia, Spain.

framework for generating cognitive SA, blending elements from physical, cyber, and psycho-social domains, emphasizing its operational and tactical application for multi-domain environments. The paper addresses the challenges in visualizing cognitive SA, advocating for the correlation of diverse data sources, including social network monitoring, to enrich cognitive SA. This work complements Burda's by providing a detailed framework for generating and visualizing cognitive SA, making use of modern technology and underscoring the necessity of sophisticated tools and methods to navigate the complex landscape of cognitive warfare.

A third paper expanding on digital tools, situational awareness and visualization is Nitin Agarwal's[12] "Developing Socio-computational Approaches to Mitigate Socio-cognitive Security Threats in a Multi-platform Multimedia-rich Information Environment". Agarwal's paper delves into the growing weaponization of social media, highlighting how it influences strategic, operational, and tactical military operations. Agarwal specifically addresses the phenomenon of 'flash event style' cognitive threats, including deviant cyber flash mobs and the rapid spread of misinformation. The paper also provides a framework for understanding and mitigating these threats, focusing on characterizing information actors and their tactics, which is vital for developing countermeasures. Agarwal's work further explores the exploitation of algorithmic biases in social media platforms, a crucial aspect of modern cognitive warfare. The study's emphasis on collective action in cyber campaigns and the identification of focal structures within social networks for effective cognitive attack mitigation provides practical insights into the operationalization of cognitive warfare defence strategies. This approach complements Domingo's framework for visualizing cognitive SA and Burda's argument for the integration of AI and ML in defence strategies against cognitive warfare. It highlights the need for advanced tools and methodologies to detect, analyse, and mitigate the sophisticated tactics employed in modern cognitive warfare, as well as the need for sophisticated data integration and visualization methods.

Embarking from this SA-visualisation and computer technology perspective, other papers offer different perspectives on the use of technologies in cognitive warfare. For example, Øyvind Voie's[13] paper "Human Enhancement Technologies and the Possible Dual Use in Cognitive Warfare" explores emerging frontiers in genome editing and brain-computer interfaces (BCIs), discussing their implications in cognitive warfare. The paper delves into the dual-use dilemma of these technologies: their potential to enhance human cognition and health versus their weaponization. It emphasizes that while genome editing could modify genetic sequences to enhance cognitive function, it could also be used malevolently, such as creating genetically superior individuals or degrading adversaries' cognition. Similarly, BCIs, enabling direct brain-device communication, could amplify cognitive abilities like memory or learning but also be exploited for information theft or manipulation. The paper underscores the need for societal and technological safeguards against their misuse in cognitive warfare, balancing their benefits with ethical considerations.

Similarly, Enrique Martín and Valarie Yerdon's[14] "Cognitive Augmentation for Military Applications" grounds the vision, focusing on cognitive enhancement technologies in military settings. It explores the potential of technologies like neurostimulation and brain-computer interfaces to augment cognitive capabilities crucial in cognitive warfare. The paper analyses various methods and tools that could enhance human performance, with an emphasis on neurotechnologies and their expected impact by 2040. It also delves into the Ethical, Legal, and Social Issues (ELSI) associated with these technologies, advocating for a global perspective that goes beyond Western views. This work complements Øyvind Voie's paper on the dual-use dilemma, sharing a focus on the potential and risks of cutting-edge technologies. Both papers highlight the ethical considerations and the necessity of safeguards against misuse in cognitive warfare, underlining the importance of balancing technological advancement with responsible application in military and civilian spheres.

[12] Nitin Agarwal, COSMOS Research Center at University of Arkansas – Little Rock, USA.

[13] Øyvind Voie and Susanne Glenna, the Norwegian Defence Research Establishment (FFI), Norway.

[14] Enrique Martin, E&Q Engineering, Spain; and Valarie Yerdon, Thor Solutions LLC, USA.

Another perspective offered is Cassandra Granlund's[15] paper "Chemicals in Cognitive Warfare: A Peek Inside the Mind-Modifying Arsenal", which addresses the use of chemicals and pharmaceuticals as neuroweapons in cognitive warfare. It reviews various agents, from toxic industrial chemicals to pharmaceutical-based agents, highlighting their potential to manipulate human cognition and behaviour. The paper discusses the historical use of substances in warfare for incapacitation or cognitive enhancement, emphasizing the evolving nature of cognitive warfare. It also explores the potential misuse of neuroscience and technology in creating novel neuroweapons and the ethical concerns associated with their development and deployment. Granlund stresses the importance of understanding these potential threats to develop countermeasures and defensive strategies, emphasizing the need for ongoing research and international collaboration to address the challenges posed by chemical agents in cognitive warfare.

These three papers illustrate the double-edged nature of novel technologies. They highlight the potential for technological advancements to be exploited in cognitive warfare. Together with Burda, Aragonés *et al.*, and Agarwal these papers underscore the multifaceted nature of cognitive warfare: from cyber-based psychological manipulation (Agarwal and Aragonés) to the physical alteration of human cognition through emerging technologies (Voie) and chemical agents (Granlund). This synthesis reveals a complex and evolving landscape of cognitive warfare, where diverse methods are employed to influence, manipulate, and control human cognition and behaviour. The collective insights of these papers stress the need for advanced analytical tools and comprehensive defensive strategies, as outlined by Burda, to navigate and mitigate the sophisticated and diverse tactics employed in modern cognitive warfare.

2.3.1 Notes from Discussions

Technological and societal aspects formed a significant part of the cognitive warfare discussions, with emphasis on the sharing of research from national levels to NATO, including questions of funding, expert teams, and collaborative efforts. The complexities and challenges in using technology, including adapting to social media tools' changing rules and understanding cultural contexts, were highlighted, indicating the dynamic interplay between technology and societal factors in cognitive warfare. The need for regulations and strategies for emerging technologies was also aptly underscored, reflecting the ongoing evolution and complexity in the application of cognitive warfare principles.

2.4 Strategies and Models for Cognitive Warfare

Cognitive warfare demands innovative strategies and models for effective defence and resilience. This section of papers explores unique insights and methods geared towards understanding and countering cognitive warfare. The papers collectively offer a multi-dimensional perspective, ranging from theoretical frameworks to practical models, emphasizing the importance of a comprehensive, whole-of-society approach in this domain.

In "Calibrated Trust as a Means to Build Societal Resilience Against Cognitive Warfare," Esther Kox, Neill Bo Finlayson, Julia Broderick-Hale and José Kerstholt[16] articulate a compelling framework emphasizing the pivotal role of trust in defending against cognitive warfare. They dissect the complexities of trust dynamics in the context of cognitive warfare, describing how strategic manipulation of information aims to erode societal trust. The paper introduces the concept of calibrated trust, involving a cycle of building, managing, and repairing trust, which is crucial for maintaining societal resilience balancing a healthy level of distrust or scepticism with trust. This well-received work underscores a whole-of-society approach, offering insights for policymakers and practitioners. Its focus on trust calibration as a defensive strategy against cognitive warfare sets a foundational perspective for understanding and countering such threats.

[15] Cassandra Granlund, the Norwegian Defence Research Establishment (FFI), Norway.

[16] Esther Kox, Neill Bo Finlayson, Julia Broderick-Hale, and José Kerstholt, Netherlands Organisation for Applied Scientific Research (TNO), The Netherlands.

Complementing this, L. Bjørgul and S. R. Sellevåg's[17] paper "Scenarios as a Tool to Increase Resilience Against Foreign Influence: A Norwegian Example," delves into the use of scenario development, particularly general morphological analysis, to predict and counter cognitive warfare tactics. This method, in this case used within the context of the Norwegian electoral cycle, categorizes possible scenarios of election interference and emphasizes the need for tailored national approaches. While Kox's paper highlights the significance of trust calibration in societal resilience, Bjørgul and Sellevåg's work advocates for proactive scenario planning, suggesting a synergy between these strategies. Both papers collectively advocate for a comprehensive, whole-of-society approach to cognitive warfare, blending theoretical insights with practical methods for broader and more effective resilience building.

Silje Lensu Dåbakk's[18] paper, "Mitigation through Simulation: An Evaluation of the Somulator Social Media Training Tool in the Norwegian Armed Forces," adds a practical dimension to this synthesis. It evaluates the effectiveness of simulated social media environments in training military personnel to counter cognitive warfare. The Somulator tool provides realistic scenarios for personnel to experience and respond to cognitive warfare tactics, enhancing situational awareness and strategic communication skills. This practical approach to training dovetails with the theoretical and strategic insights of Kox and Bjørgul, showcasing how simulation-based training can complement trust calibration and scenario planning to build a comprehensive defence against cognitive warfare.

The exploration of these three papers reveals a complex and layered approach to cognitive warfare, encompassing trust dynamics, scenario planning, and simulation training. Each paper contributes a unique piece to the puzzle, collectively building a robust framework for understanding and responding to cognitive warfare. The synthesis of these works underscores the necessity of integrating theoretical knowledge with practical applications, emphasizing a holistic, multidisciplinary approach. This comprehensive view is crucial in the evolving landscape of cognitive warfare, ensuring readiness and resilience against these emerging challenges.

2.4.1 Notes from Discussions

The discussions around these papers revolved around the role of trust and narratives within NATO and the building of resilience. The need for training interventions to build resilience, including scenario-based training, was highlighted, along with the challenges of training people to remove biases. This discussion points to the strategic and systemic considerations necessary in developing effective cognitive warfare defences. Furthermore, the adaptability of tools like the Somulator for civilian exercises was discussed, pointing to the practical aspects of cognitive warfare training.

2.5 Cognitive Warfare in the Field and in Practice

The final category of papers presented at the symposium centred on the more practical aspects of the topic. Included here are papers devoted to fieldwork studies, experiments and the real-world context to cognitive warfare.

The paper by J.L. Albert Martínez, A.A. Garcia Juan, C. Martinez Bernalt, J.M. Valdés de Olives and S. Fernández Juin[19] "Information environment analysis and its role in combating influence operations: The example of the Russian invasion of Ukraine", discusses the strategic use of disinformation campaigns by Russia, emphasizing the transformative role of social media and digital platforms in modern conflict. This study highlights the necessity of comprehensive information environment analysis, demonstrating how

[17] Lea Bjørgul and Stig Rune Sellevåg, the Norwegian Defence Research Establishment (FFI), Norway.

[18] Silje Lensu Dåbakk, the Norwegian Defence Research Establishment (FFI), Norway.

[19] J.L. Albert Martinez, A.A. Garcia Juan, C. Martinez Bernalt, J.M. Valdés de Olives, and S. Fernández Juin, Joint Chiefs of Staff of the Armed Forces, Spain.

strategic communication and understanding of cognitive tactics are essential in identifying and countering influence operations. The work lays a foundational understanding of the macro-scale strategies employed in cognitive warfare, emphasizing the need for sophisticated methodologies in strategic communication to maintain integrity in decision-making processes.

Expanding on the themes of narrative manipulation and strategic communication, the paper "How China Conducts Influence Operations by Leveraging Culturally Nuanced Narratives in Three Southeast Asian Countries" by Peggy-Jean M. Allin, Steven R. Corman, Charmaine Misalucha-Willoughby, Elena Steiner, Mark Woodward and Scott Ruston[20] explore China's sophisticated use of culturally nuanced narratives in Southeast Asia. Their study, focusing on influence operations in the Philippines, Malaysia, and Indonesia, illustrates China's strategic adaptation of its narratives to suit each country's unique cultural and political landscapes. This approach not only complements the previous paper's findings on the strategic use of disinformation but also adds a critical dimension of cultural sensitivity and adaptability. The paper underscores the importance of understanding the target audience's cultural context as a key element in the success of cognitive warfare strategies.

Remaining in the Asian context, Arild Bergh's[21] paper "Being There: Content, Cognition and Strategic Competition" ties directly into the themes above. Bergh argues that the absence of relevant, authoritative content in digital media creates a vacuum that can be exploited by adversarial influence operations. This is illustrated by his recent fieldwork in Okinawa, Japan. His emphasis on proactive and creative content generation as a countermeasure to such operations connects to the earlier discussions on narrative manipulation. Bergh's work underscores the tactical aspect of cognitive warfare, highlighting the need for democracies to actively engage in the information environment to combat the influence of adversarial narratives.

Moving slightly more into the experimental arena, Stefano Menicocci, Viviana Lupo, Silvia Ferrara, Andrea Giorgi, Gianluca Borghini, and Fabio Babiloni's[22] study on the psychological and behavioral aspects of individuals' interactions with fake news is related in their paper "Fake news attitude recognition: how users' behavioral and implicit components change based on conscientiousness and visual attention." The paper provides a crucial link to the individual level of cognitive warfare. By exploring the role of personality traits like conscientiousness and visual attention in discerning fake from real news, this work bridges the gap between high-level strategies and their cognitive reception. This study is particularly relevant in the context of the narrative manipulation strategies discussed by the earlier papers in this category, as it sheds light on the effectiveness of these tactics at an individual level. Their findings highlight the importance of understanding individual cognitive processes as part of the broader strategy to counter cognitive warfare tactics.

In "The Fog of War: An Avenue to Explore Vulnerabilities and Mitigating Measures to Cognitive Warfare," by Sebastian Cancino Montecinos and Per-Erik Nilsson[23], the focus is on understanding cognitive warfare in extreme conditions and its impact on sense-making abilities, particularly during wartime. This is placed in

[20] Peggy-Jean M. Allin, Center on Narrative, Disinformation and Strategic Influence, Arizona State University, USA; Steven R. Corman, Center for Strategic Communication, Arizona State University, USA; Charmaine Misalucha-Willoughby, De La Salle University, the Philippines; Elena Steiner, Center on Narrative, Disinformation and Strategic Influence, Arizona State University, USA; Mark Woodward, Center for the Study of Religion and Conflict, Arizona State University, USA; and Scott Ruston, Center on Narrative, Disinformation and Strategic Influence, Arizona State University, USA.

[21] Arild Bergh, the Norwegian Defence Research Establishment (FFI), Norway.

[22] Stefano Menicocci, Sapienza University of Rome, Department of Molecular Medicine; Viviana Lupo, Sapienza University of Rome, Department of Molecular Medicine; Silvia Ferrara, Brainsigns srl.; Andrea Giorgi, Sapienza University of Rome, Department of Anatomical, Histological, Forensic and Orthopaedic Sciences; Gianluca Borghini, Sapienza University of Rome, Department of Molecular Medicine; and Fabio Babiloni, Sapienza University of Rome, Department of Molecular Medicine, Italy.

[23] Sebastian Cancino Montecinos, and Per-Erik Nilsson, Swedish Defense Research Agency (FOI), Sweden.

the context of the full-scale invasion of Ukraine by Russia and is tied to the experience of war. The paper emphasizes the heightened susceptibility of civilians and military personnel to cognitive warfare tactics due to mental fatigue and limited access to reliable information in conflict zones. It proposes a framework for studying the influence of external stimuli on cognition under such conditions, aiming to develop strategies to mitigate cognitive warfare's effects. This is another example of real world considerations in cognitive warfare.

In summary, the synthesis of these papers provides a comprehensive picture of cognitive warfare in the field and in practice. From analysis of large-scale, strategic influence operations to Menicocci et al.'s exploration of individual cognitive responses on the tactical level, these studies collectively underscore the multi-layered nature of cognitive warfare. They highlight the necessity for a multifaceted approach that encompasses not only the understanding and countering of strategic narratives and disinformation but also the importance of content creation and the recognition of individual psychological patterns. This holistic view is crucial for effectively responding to the complex challenges posed by cognitive warfare in the modern information landscape.

2.5.1 Notes from Discussions

The conversation on fieldwork and practicalities in cognitive warfare highlighted the multifaceted nature of understanding the "will to fight," indicating the necessity for nuanced strategies. This aspect is pivotal in understanding cognitive resilience and response in conflict situations. It was also noted that fieldwork presents unique challenges, notably influenced by Covid-19 and logistical constraints, emphasizing the critical role of culture-specific knowledge. A deeper understanding of national characteristics through social research underscores the complexities in fieldwork execution. The discussion extended to the nuances of cognitive warfare in gray zones and during war, with legal and ethical implications coming to the fore, suggesting a potential alignment with cyber warfare strategies. The lack of a cohesive "western" narrative against strong strategic narratives from adversaries like Russia was also a point of focus.

3.0 CONCLUSIONS

The HFM-361 Symposium marked a significant step in NATO's approach to understanding and addressing cognitive warfare. This event brought together a wide range of experts from different fields, showcasing the varied approaches and insights that are essential in tackling the complexities of cognitive warfare. The symposium demonstrated the depth and diversity of expertise available, highlighting the many ways to conceptualize and respond to these challenges. The event was instrumental in fostering conversations that bridge these diverse viewpoints, creating room for collaboration and mutual understanding among experts from different backgrounds.

This marks both an opportunity and a challenge for the scientific community. On the one hand, the broad approach shows the varied toolkit available to not only understand the phenomenon, but also to counter, mitigate and defend against it. On the other hand, this broadness sows the ground for misunderstanding and confusion among different disciplines, where terms and ideas may be used differently. The implication of this duality is hopeful: there is ample opportunity to learn a lot about cognitive warfare and to build mechanisms that defend against it, but this will require careful and methodical progress.

Partly related, the Symposium also highlighted the constantly changing nature of cognitive warfare. The presentations and discussions showed that an adaptable and multifaceted approach is necessary to keep up with evolving threats. The combination of social science perspectives, as seen in Goolsby's and Forrester's works, with the more technical aspects brought to the fore by Ask and Flemisch, demonstrated the need for a comprehensive strategy that includes a variety of methodologies and insights. This supports the idea of a slow and steady approach that utilizes the breadth of knowledge possessed.

Moreover, the symposium brought attention to the ethical dimensions of cognitive warfare. The discussions, particularly those on the dual-use dilemma of certain technologies, emphasized the importance of considering the moral implications of advancements in this field. Balancing the potential benefits of these technologies with ethical concerns is crucial to ensure that efforts in cognitive security do not inadvertently cross ethical boundaries. This is of particular importance in this time rapid development of groundbreaking technologies such as machine learning and artificial intelligence.

In summary, the HFM-361 Symposium contributed significantly to the common understanding of cognitive warfare within the NATO scientific community. It provided a platform for sharing research and ideas, and for experts from different areas to learn from each other. The event, combined with other research activities on the topic within NATO STO, represents important steps towards a more mature understanding of cognitive warfare. The insights gained from this symposium will be crucial in developing effective strategies to deal with the complex challenges of cognitive warfare in the future. The path is wide, but the going should be slow.

4.0 RECOMMENDATIONS FOR FUTURE WORK

Cognitive warfare is not yet a fully understood phenomenon enjoying deep consensus, indeed the field requires future work in nearly all disciplines in order to mature. This future work should include cross-disciplinary and cross-national initiatives, which to a greater degree will strive to create connections that cement cognitive warfare as a known entity among partners.

The emergence of new technologies, like brain-computer interfaces or rapid advances in the field of AI are certain to have major impacts on war in general and cognitive warfare in particular. Research needs to keep abreast of these developments, and it may be safer to be more speculative than more conservative, in order to make sure one does not suffer the failure of imagination that often befalls those looking into the future.

Future research directions could include exploring the ethical implications of cognitive warfare, particularly in the use of AI and neuromodulation technologies. The establishment of international norms and regulations governing the use of cognitive warfare tactics will also be critical. Furthermore, understanding the impact of cognitive warfare on civilian populations and developing methods to protect against such warfare tactics will be paramount.