The Understanding of Cognitive Warfare in Comparative Perspective Taking Stock and Bridging the Gap to Extant Literatures

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

christoph.deppe@hsu-hh.de

ABSTRACT

Cognitive Warfare is an emerging concept subject to discourses in military and academic spheres. For effective communication and constructive research, the mutual intelligibility between different research areas is paramount. This work contributes to the intelligibility of different areas of Cognitive Warfare research by examining the Cognitive Warfare concept in military and scientific publications and investigating the relation of the Cognitive Warfare concept to the neighboring concepts Hybrid Threats and Foreign Information Manipulation and Interference.

1.0 INTRODUCTION

Cognitive Warfare is a novel concept that aims to address the exploitation of human cognition and technology to disrupt, undermine, influence, or modify human decision-making see [1], [2], [3]. It has become increasingly relevant in the current security environment, where adversaries continuously seek to undermine the integrity of political processes in democratic societies, as well as their military-strategic objectives, by deploying sophisticated strategies through coordinated political, military, economic, and information efforts see [4], [5], [6]. Cognitive Warfare achieves overt and covert objectives below and above the threshold of war, affecting how we think, act, and make decisions, as well as our (shared) perception of reality.

This paper aims to investigate three neighboring concepts - Foreign Information Manipulation Interference (FIMI), Hybrid Threats, and Cognitive Warfare– which partly lack exhaustive definitions and are continuously evolving within different institutional spheres. Institutions tend to frame political discourse by defining acceptable discursive interactions, which reflects their interests and values [7]. Furthermore, concepts developed by institutions to fulfill a certain non-academic function, like military concepts, can differ from concepts in the social scientific realm [8], [9], [10]. Moreover, existing concepts that are tasked with encompassing additional cases or phenomena due to institutional or analytical demands are susceptible to conceptual stretching or travel, presenting its own challenges [11]. In sum, this warrants an investigation of novel concepts, their analytic capacity, and their relation to existing scientific concepts and literature. The concepts of FIMI, Hybrid Threats, and Cognitive Warfare exhibit several overlapping attributes. The lack of clearly defined intensions and extensions of these concepts may hinder the understanding of their functional differences, analytic capacity, and interoperability [8]. Academic research and NATO are connected to gain intellectual, conceptual, and epistemological superiority. Therefore, it is of utmost importance to be aware of conceptual mismatches between academic and NATO (military) concepts. We refer to the discursive institutionalism by Schmidt to differentiate between two different causal explanations of mismatches: a) different academic conceptions and b) different institutional logics, which overpower academic conceptions [12], [13]. The later could hamper the above-mentioned superiority resulting from the connection between academia and NATO.

This leads to three main research questions. Firstly, does the Cognitive Warfare Concept by NATO ACT offer analytical capacities from a political science standpoint, or is its primary utility confined to institutional military applications? Secondly, how is Cognitive Warfare conceptualized and represented in scientific literature? Finally, what are the functional and analytical disparities in comparison to neighboring concepts, namely FIMI and Hybrid Threats and how are the three concepts related?

The paper proceeds as follows: In section 2 the Cognitive Warfare concept by NATO ACT [14] is discussed in detail. One analytic focus of the section is the institutional function that the concept is aimed to fulfil. In section 3 the Cognitive Warfare (also cognitive conflict and cognitive domain) concept in scientific literature is analyzed at length. The section introduces a periodization of the emergence of Cognitive Warfare in scholarly discourse, as well as a categorization and discussion for different definitions of Cognitive Warfare. The section concludes by discussing shortcomings and research gaps in the existing literature on Cognitive Warfare. Section 4 is focused on the relation of the Cognitive Warfare concepts to the closely related concepts FIMI and Hybrid Threats. The analysis is conducted in two steps. First the concepts are analyzed with a supervised linguistic analysis based on reference documents. In a second step a brief concept comparison follows. The section combines two different approaches to concept comparison to deliver a nuanced analysis. Section 5 concludes the paper by presenting the results and addressing the research questions.

2.0 THE COGNITIVE WARFARE EXPLANATORY CONCEPT

Over the past two decades, the delineations between peace and conflict have become increasingly indistinct. In the same time period, a rapid change fueled by technological innovation has radically transformed the way individuals, groups, institutions, and whole societies communicate, how they produce and consume information. This transformation, along with changes in economic systems, the global security environment and other factors, has made it necessary to develop new academic and military concepts to make sense of and analyze novel forms of competition and conflict situation. These concepts include unconventional warfare, hybrid threats, hybrid warfare, and FIMI, to name a few. More recently, in light of drastic changes in the global security environment and the rapid emergence of new threats in the cyber and cognitive domains, the concept of Cognitive Warfare has been introduced to academic and military discourses.[1] The effects of hybrid tactics, such as disinformation, can be observed in many democratic societies. Many activities are attributed to Russia and China. Recently, a prominent case of state intervention in democratic proceedings was the Russian involvement in the 2016 U.S. presidential election, favoring Republican candidate Donald J. Trump. The specifics of Russian action during this election were outlined in a report compiled by Special Counsel Robert Mueller [15]. The report meticulously catalogues Russia's interference, which was orchestrated through operations orchestrated by the Internet Research Agency (IRA).

2.1 The Purpose of the Cognitive Warfare Concept

In the 2022 Strategic Concept [16] NATO highlights activities by Russia and China as significant threats to the Alliance's security and interests. It points out that Russia employs tactics such as coercion, subversion, aggression, and annexation to establish spheres of influence and direct control. The country utilizes a combination of conventional, cyber, and hybrid means against NATO and its partners. Regarding China, the strategic concept notes that its stated ambitions and coercive policies challenge NATO's interests, security, and values. China employs various political, economic, and military tools to expand its global presence and assert influence. However, it maintains opacity about its strategy, intentions, and military build-up. The strategic concept 2022 states that China's aggressive use of hybrid and cyber operations, along with its confrontational rhetoric and dissemination of disinformation, target Allies and pose a threat to Alliance security.

[1] See Section 3 for a periodization of the emergence of Cognitive Warfare in scholarly discourse, as well as a categorization and discussion for different definitions of Cognitive Warfare.

The strategic concept also recognizes the escalating threat of hybrid tactics [16]. These tactics encompass a spectrum of measures, including political, economic, energy, and informational methods, employed coercive to attain strategic goals. Notably, there is an acknowledgment that hybrid operations against Allies can escalate to the level of an armed attack, potentially necessitating the invocation of Article 5 of the North Atlantic Treaty [17]. Consequently, NATO aims to improve its capabilities for preparedness, deterrence, and defense against the coercive application of hybrid tactics, by state or non-state actors. The strategic concept also states, that the Alliance will maintain its support for partners in countering hybrid challenges, striving for optimal collaboration with relevant institutions like the European Union. From this brief analysis of the strategic concept, one of the most important policy documents for NATO, it can be concluded, that hybrid tactics and related activities are a severe factor to NATO, which demands adequate responses. The NATO Warfighting Capstone Concept (NWCC) is subordinate to the strategic concept and is a military concept that outlines NATO's vision for maintaining and developing its military advantage through 2040 [18]. It addresses the changing character of war and power competition, and emphasizes the need for NATO to be able to operate in all domains, including space and cyberspace. The NWCC also highlights the importance of interoperability and partnerships with other nations and organizations. The NWCC defines "6 Outs", which are a set of functions that the future Alliance MIoP (Military Instrument of Power) must aspire to outperform to maintain NATO's military advantage. These functions are: out-think, out-excel, out-fight, out-pace, out-partner, and out-last ([18], pp. 10-11). The idea is that by excelling in these areas, NATO will be better able to understand and respond to potential adversaries, foster partnerships, and adapt to changing circumstances. The resulting warfare development imperatives are five key areas that NATO must focus on to achieve these goals. These imperatives are: cognitive superiority, layered resilience, influence and power projection, cross-domain command, and integrated multi-domain defence ([18], p. 12).

Within the five warfare development imperatives listed in the NWCC, Cognitive Warfare is most relevant in the area of cognitive superiority. Cognitive superiority describes the ability of NATO to better understand the operating environment and potential adversaries relative to its own capabilities and objectives ([18], p. 14). It involves expanding knowledge and understanding across all domains, enabled by technology, to maximize the ability of military leaders to anticipate, think, decide, and act. The goal is to achieve cognitive advantage over potential adversaries by building better situational awareness and understanding. The Cognitive Warfare Concept within NATO serves a twofold purpose: to improve the comprehension of evolving threats within the cognitive realm and to lay the groundwork for potential future developments in warfare in the cognitive domain ([14], p. 7). The concept shall provide a unified framework for comprehending and effectively addressing Cognitive Warfare, outlining its dynamics, mechanisms, and implications for both NATO's warfighting capabilities and cognitive superiority. Its overarching objective is to improve NATO's cognitive resilience, as well as to protect and enhance decision-making capacities.

In essence, the Cognitive Warfare Concept shall enhance NATO's understanding of upcoming cognitive threats, protect cognitive resilience by defining potential impacts, and produce a holistic strategy for mitigating the effects of Cognitive Warfare through tactics like education, collaboration, protection, and influence in the cognitive domain. This concept thus fulfills a distinct role as a lower-level military concept, positioned subordinate to the NWCC. In due course, the aspiration is for the Cognitive Warfare concept to be integrated into NATO's official doctrine [19].

2.2 The Cognitive Warfare Exploratory Concept

In this chapter, the Cognitive Warfare Exploratory Concept [14] is reviewed from a methodological perspective form the social sciences. For this analysis only the conceptually relevant elements of the Exploratory Concept are considered.

The definition, use, and significance of concepts in social science is a complex and contested research area in the social sciences [8], [9], [20]. In its basic form, a concept consists of a term, that names the concept; one or more empirical referents, that are captured by the concepts, thereby defining the denotation or extension

of a given concept; and lastly, one or more defining attributes, that fill the concept with meaning, defining the connotation or intension of a given concept.[2] Gerring ([9], pp. 40-46) described eight criteria for the evaluation of conceptual goodness: coherence, operationalization, validity, field utility, resonance, contextual range, parsimony and analytical/empirical utility, which will be used for the evaluation of the Cognitive Warfare concept in section 2.3. It is important to note that the Cognitive Warfare concept has been developed as a military concept, to fulfill specific institutional functions. Also, the practice and aim of military concept development in NATO [10] differs greatly from concept development in the social sciences. While military concepts usually describe new capabilities in the military context, social science concepts aim to produce analytically valuable building blocks, which can be connected to existing theories and be integrated in feasible research designs. Despite of these significant differences in conceptual design and aim, it is paramount to evaluate concepts from different domains, to ensure intelligibility in the broader discourse, even if this demands the reconceptualization of a given concept for the application in social science.

2.2.1 Basic Concept and Definition

The review of the Cognitive Warfare concept begins at the highest level, with the concept term and the basic definition. The proposed definition of Cognitive Warfare as published in the exploratory concept by NATO ACT is “Activities conducted in synchronization with other Instruments of Power, to affect attitudes and behavior by influencing, protecting, or disrupting individual and group cognition to gain advantage over an adversary” ([14], p. 3).

The substantive necessity for a concept like Cognitive Warfare is derived from observed challenges for NATO, which can be broken down into two developments. First, technological progress and shifts in information consumption, wield adversaries’ greater capacity to amass and manipulate data, sway emotions, and shape beliefs and behaviors. This enables the leveraging of societal divisions through the use of technologies (e.g., artificial intelligence (AI), emerging & disruptive technologies, data harvesting), and the proliferation of social media influencing individuals’ thoughts, emotions, and actions. As the authors themselves state, this mirrors hybrid warfare tactics, where adversaries target society as the vector to exert influence indirectly on key targets: political and military leaders. The effectiveness of influence campaigns is conceptualized to hinge on the calculated manipulation of emotions and cognitive predispositions to instigate widespread shifts in attitudes and behavior. These alterations are frequently nuanced, blurring the distinction between genuine societal debate and discord, and the hostile exploitation of societal divisions through cognitive attacks ([14], pp. 7-8).

Second, it is stressed that cognitive attacks are not new, however the Concept defines them as deliberate offensive maneuvers aimed at influencing perceptions, beliefs, interests, decisions, and behavior by directly targeting the human mind. It is conceptualized that the innovation is the capacity of adversaries to swiftly and anonymously execute these cognitive attacks within the Information Environment (IE) through digital platforms and emerging disruptive technologies (EDTs) ([14], p. 8).

Especially the focus on cognition and the human mind distinguishes the Cognitive Warfare concept from other concepts like Hybrid Threats, FIMI and disinformation, whose conceptualized effects often end at the acceptance or rejection of specific information or narratives. In the concept of Cognitive Warfare, the main effect is conceptualized to lie in the manipulation of emotional and subconscious processes of the human mind and therefore much more far-reaching than in other concepts. The authors clarify that, “synchronized and coordinated attacks on emotions, thoughts and behaviors impact will, morale, decision-making and situational understanding” ([14], p. 13). Furthermore, “Cognitive attacks are designed to use information to activate the subconscious processes in our brains, making it difficult for our conscious minds to perceive the presence of a cognitive threat” ([14], p. 14). These factors constitute an approximation to the empirical referents that partly constitute the extension of the concept.

[2] This model is also known as the Ogden-Richards Triangle for a detailed discussion see [20].

2.2.2 Problem Space

The problem space section of the explanatory concept provides an overview of the problem of Cognitive Warfare, again adding to the empirical referents of the concept. It begins by labeling Cognitive Warfare to be a value-neutral set of tactics, which can be employed at every stage on the continuum of competition. It is furthermore problematized as a Whole-of-Society Problem in which "adversaries are targeting the NATO Alliance through campaigns to malignly influence the attitudes, decisions and behaviors of individuals, groups and societies. Emerging and Disruptive Technologies (EDTs) and sciences enable these cognitive attacks. Our adversaries aim to turn our strengths into vulnerabilities that weaken the Alliance" ([14], p. 17) In this definition the role of technological innovations in the distribution of influence campaigns is highlighted as a powerful enabling factor, that can be used to attack the discourse spaces of open liberal democratic societies. Furthermore, the Military Challenge of Cognitive Warfare is described as "Alliance decision-making, mission and forces are directly and indirectly vulnerable to cognitive attacks. The role of the Military Instrument is the cognitive dimension is unclear, particularly below the threshold of armed conflict. This causes gaps in policy, defence planning and capabilities" ([14], p. 17). Hereby, the concept is connected to ongoing discussions in many democratic societies, about the role of different governmental institutions in the mitigation of threats in the information environment.[3]

Next, the kind of actions, that are considered to be part of Cognitive Warfare are listed. These tactics, or vectors and enablers can be considered to be the defining attributes that constitute the meaning or intension of the Cognitive Warfare concepts. Cognitive attacks, both presently and potentially in the future, are described to be facilitated through a range of vectors, capabilities, and enablers. These encompass:

- **Traditional Vectors and Enablers** ([14], p. 19): This category includes kinetic force and established channels like broadcast and print mass media. Additionally, it involves various actors such as corporate, state, and political entities, along with interpersonal engagement.
- **Existing Technology Vectors and Enablers** ([14], p. 19): This domain leverages contemporary technology. It encompasses social media platforms, the utilization of big data, the integration of augmented reality and wearable smart devices, as well as the use of gaming and encrypted communication platforms. Avatars and virtual profiles are also instrumental in this context.
- **Emerging Technology Vectors and Enablers** ([14], p. 19): This category delves into cutting-edge technologies that hold significant potential for cognitive attacks. It encompasses synthetic media, exemplified by deepfakes and AI-driven media. Additionally, it includes the widespread use of artificial intelligence, the immersive realm of the Metaverse, and the concerning emergence of neuroweapons. The listed vectors and enablers encompass a wide spectrum of tactics and approaches, underscoring the wide intension of the Cognitive Warfare concept.

Further, the concept identifies various individual risk factors and resulting triggers that heighten susceptibility to micro-level cognitive attacks ([14], pp. 24-26). These include deficiencies in accurate knowledge, deeply ingrained worldviews, negative emotional experiences, and limited literacy. Addressing these factors is crucial for enhancing the resilience of both NATO personnel and member nations against cognitive attacks. This can be achieved by improving knowledge, critical thinking, and emotional resilience. Additionally, the document outlines three primary triggers influencing vulnerability to influence and manipulation. These are cognitive inflexibility, the need for social belonging, and emotional arousal. Mitigating these triggers is vital for bolstering resilience against cognitive attacks. This involves promoting cognitive flexibility, fostering a sense of belonging, and managing emotional arousal.

The concept also names risk factors that heighten vulnerability to cognitive attacks on the meso-level i.e., in social and cultural groups ([14], p. 26). These factors include group polarization and social trust. Group polarization, influenced by human social tendencies, can be exacerbated by social media platforms through

[3] Also see STO activity SAS-177 "Defending Democracy in the Information Environment – Foundations and Roles for Defence": https://www.sto.nato.int/Lists/test1/activitydetails.aspx?ID=17185

algorithms that reinforce existing beliefs. This fosters confirmation bias and the spread of disinformation, undermining trust and manipulating groups. Social trust, crucial for societal cohesion, can be exploited by malign actors spreading disinformation to erode trust in institutions and leaders. Addressing these risk factors is crucial for enhancing the resilience of NATO personnel and member nations against cognitive attacks. This can be achieved by promoting critical thinking, bolstering social trust, and countering group polarization.

Finally, the concept also examines risk factors on the macro level, i.e., societies and nations. It illuminates nations' varying susceptibility to cognitive attacks, a crucial consideration for NATO in evaluating member nations' resilience. While NATO's Military Instrument of Power (MIoP) does not possess a direct mandate to address these factors, their understanding remains essential. They are conceptualized as the basis for collaborative efforts with NATO partner nations and non-NATO organizations.

In liberal democracies, a notable vulnerability exists to adversarial Cognitive Warfare, challenging NATO's foundational values ([14], p. 27). While preserving the liberal democratic system remains a priority, it is recognized as a risk factor due to the principled rejection of authoritarian control methods. Adversaries perceive this as a significant vulnerability that can be exploited to sow discord within societies and erode the ability to govern in line with liberal democratic principles.

Information and Media Literacy is underscored by research, indicating a direct correlation with susceptibility to disinformation and cognitive manipulation ([14], p. 27). Safeguarding civil society from cognitive attacks is important from a military defense standpoint, recognizing that even NATO personnel may be affected by insufficient information and media literacy. Citizens, including NATO personnel, often remain unaware of their vulnerabilities to cognitive manipulation, underscoring the necessity for heightened information and media literacy efforts.

Civic Engagement encompasses activities that enhance community well-being through political and non-political means, breaking down barriers and augmenting societal resilience ([14], p. 27). While improving civic engagement falls beyond NATO's political and military scope, recognizing its protective potential offers an opportunity for the Alliance to collaborate with external entities focused on fortifying societal resilience.

NATO has observed a surge in anti-establishment populism, indicating discontent with prevailing economic, social, and cultural conditions in numerous NATO member nations ([14], p. 27). In some instances, the growing support for populist ideologies may also signify the influence and success of cognitive attacks by adversaries. These are achieved through various means, including espionage, hacking, disinformation campaigns, and covert funding of political movements.

From a methodological viewpoint, the risk factors for an increased vulnerability to cognitive attacks on the micro, meso and macro levels, listed above, can potentially be attributed to be part of the extension of the concept. This is because these factors can be read as a list of variables, that constitute a case, that would be captured by the concept Cognitive Warfare. From the counter perspective, if a given hypothetical case featured none of the listed risk factors, it would not be captured by a measurement that captures instances of Cognitive Warfare.

In a subsequent section, the Exploratory Concept provides a list and description of the intended effects of Cognitive Warfare ([14], pp. 28-29). Cognitive warfare is conceptualized to entail a diverse range of intended effects, posing intricate challenges in recognizing attacks and their protracted consequences. In this context, cognitive attacks are employed within broader geopolitical strategies to hinder decision-making processes, erode national or institutional unity, sow societal division, exploit identities and narratives, and undermine the resolve to engage in conflict.

First, under "Impede Decision-Making and Disrupt OODA Loop," ([14], p. 28) decision-making, contingent on information availability, becomes susceptible to manipulation by state and non-state actors. Disinformation compounds uncertainty or propagates false narratives, influencing decision-makers across strata. Russia employs Reflexive Control (RC) theory to obstruct NATO's decision-making processes. Second, "Divide and Polarize Society" ([14], p. 28) pertains to deep-seated societal polarization, imperiling democracy. Adversaries exploit disinformation to systematically erode social trust, weaken institutions, and impede efforts to reconcile conflicting values and interests. This leads to societal segmentation based on various criteria. Third, "Weaponize Identity" ([14], p. 29) emphasizes the pivotal role of identity in Cognitive Warfare, influencing connections to others, societal roles, and cultural and national affiliations. Understanding the potential weaponization of identity is crucial, especially when safeguarding NATO personnel against targeted cognitive attacks. Next, "Weaponize Narratives" ([14], p. 28) highlights how historical memory and heritage significantly shape individual and group identities, influencing the narratives employed to depict how individuals, communities, and nations perceive themselves. Adversaries adeptly manipulate, discredit, and alter narratives to align with their strategic objectives. Last, "Impact the Will to Fight" ([14], p. 28) underscores that effective Cognitive Warfare requires seamless synchronization and coordination to manipulate human cognition, influencing decision-makers' comprehension of the Information Environment and their resolve to engage in conflict. Cognitive attacks introduce friction within military leadership, potentially eroding trust in NATO leadership and the overarching Alliance mission among military personnel over time.

The intended effects of Cognitive Warfare listed above can best be attributed to the intension of the concept. This is because they illustrate what an adversary seeks to accomplish by employing measures and tactics conceptualized as part of Cognitive Warfare. Analytically, "intention " is very difficult to operationalize, however, it is frequently used in related concepts like Disinformation see [21] or FIMI see [22]. This concludes the review of those areas of the exploratory concept, that are relevant to the concept specification of Cognitive Warfare from a methodological perspective.

2.3 Concept Evaluation

The subsequent section will provide a methodological summary of the Cognitive Warfare Concept as delineated in the Exploratory Concept by NATO ACT [14]. Following this, the analysis will culminate in an evaluation based on the criteria of conceptual goodness, as defined by Gerring [9].

To methodologically summarize the Cognitive Warfare Concept, the results from the review above will be allocated to the basic elements of a referential concept: The term of the concept is Cognitive Warfare, thereby clarifying that the concept describes a type of warfare happening in the cognitive domain/dimension.

The defining attributes, that fill the concept with meaning (intension or connotation) are divided in two categories. The first set of attributes that constitute Cognitive Warfare are the operations and tactics, that are considered to be part of Cognitive Warfare, which are traditional vectors and enablers, existing technology vectors and enablers as well as emerging technology vectors and enablers. The second set of attributes are the intended effects of Cognitive Warfare, which are impeding decision-making and the disruption of the Observe, Orient, Decide, Act (OODA) loop, the division and polarization of societies, weaponizing identity, weaponizing narratives and impacting the will to fight.

The concept's extension, or its empirical referents, poses a greater challenge to apprehend compared to its defining attributes. This complexity arises from the evolving nature of Cognitive Warfare and the nascent stage of many technologies outlined in the Explanatory Concept. As a result, pinpointing precise instances of Cognitive Warfare proves problematic. Consequently, a theoretical scenario of Cognitive Warfare is inferred from the Exploratory Concept. Here it can be suggested that the extension of the concept could be a series of synchronized cognitive attacks, defined as "offensive actions employed to achieve effects on perceptions,

beliefs, interests, aims, decisions and behaviors by deliberately targeting the human mind" in the Information Environment, using EDTs, in individuals, groups or societies, which are particularly vulnerable to cognitive attacks.

After summarizing the Cognitive Warfare concept, the next step involves its evaluation using Gerring's eight criteria for conceptual goodness ([9], p. 40). The first criterion is coherence, which inquires how internally coherent and externally differentiated a concept's attributes are regarding neighboring concepts ([9], p. 40). For Cognitive Warfare, the internal coherence can be considered high because the different attributes build upon each other to characterize the defined mechanisms. As far as the external differentiation goes, the concept differs from neighboring concepts in several key issues, namely the focus on cognitive effects and actions in the Information Environment using EDTs, and the sector specific focus on the military and the protection of the MIoP, the concept is therefore sufficiently coherent.

The second criterion ([9], p. 40), operationalization, probes the concept's ability to differentiate its own referents from other empirical referents distinctly. In this regard, the Cognitive Warfare concept faces a challenge as it currently lacks concrete instances in the field. Furthermore, due to the covert nature of many tactics associated with Cognitive Warfare, detecting its occurrence may be challenging. The third criterion, validity ([9], p. 40), addresses whether the concept accurately measures what it is intended to represent. In the context of the Cognitive Warfare concept, this evaluation is challenging given the absence of actual cases of Cognitive Warfare. However, it is pertinent to note that the concept is inherently future-oriented, and any present-day instances would likely be classified under different conceptual frameworks. The fourth criterion, field utility ([9], p. 40), assesses the practical usefulness of the concept in comparison to similar ones. Currently, in the realm of Cognitive Warfare, concepts like hybrid threats or information warfare hold greater analytical utility. However, as technological capacities continue to advance, Cognitive Warfare has the potential to offer a significant contribution in comprehending forthcoming threats more effectively. The fifth criterion ([9], p. 40), resonance, examines whether the concept holds relevance in both general and specialized contexts. Within NATO and military circles, the concept of Cognitive Warfare finds resonance. However, in broader non-military contexts, it may pose challenges in communication due to its explicit focus on the military sector and the term "warfare." Established concepts like hybrid threats are more likely to be employed in these scenarios. The sixth criterion ([9], p. 40), contextual range, assesses the concept's applicability across different languages. "Cognitive warfare" is a term that distinctly conveys its meaning and can be meaningfully translated. The seventh criterion ([9], p. 40), parsimony, evaluates the conciseness of the term and its list of attributes. While "Cognitive Warfare" itself is succinct and precise, its attributes are relatively extensive and may require elaboration. The eighth criterion, analytic/empirical utility ([9], p. 40), pertains to how useful the concept is in analytic contexts and research designs. In contexts focused on emerging threats, "Cognitive Warfare" holds significant analytical potential. However, the concept may have limited applicability in current empirical research applications.

2.4 Interim Results

The evaluation of the Cognitive Warfare concept based on Gerring's eight criteria for conceptual goodness reveals several insights. Firstly, the concept demonstrates high internal coherence, as its attributes synergistically characterize defined mechanisms. Additionally, it is externally differentiated from neighboring concepts by its emphasis on cognitive effects in the Information Environment using EDTs, and its specific focus on the military sector and the protection of the MIoP. However, the concept faces challenges in operationalization, as concrete instances in the field are currently lacking, and the covert nature of many associated tactics makes detection difficult. The absence of actual cases complicates validity assessment, but the concept's future-oriented nature aligns with its intent. While hybrid threats and information warfare hold greater practical utility currently, Cognitive Warfare may become increasingly relevant as technology advances. The term "Cognitive Warfare" is clear and translatable across languages. While concise, the list of attributes may require further elaboration. Lastly, in contexts focused on emerging threats, the concept holds significant analytical potential, though its current empirical applicability may be limited.

3.0 THE COGNITIVE WARFARE CONCEPT IN LITERATURE

3.1 Periodization and General Considerations

A review of publications[4] in which authors have looked extensive at the conceptual roots of Cognitive Warfare[5] results in our observation that, broadly, the concept of Cognitive Warfare has emerged in three ages, or distinct phases of conceptualization, with a fourth one currently under way[6] in which the focus appears to fall squarely on Cognitive Warfare as a valid stand-alone concept, rather than one tributary to disciplinary adjacencies.

The first age could be traced to as early as Sun Tzu and lasts until the advent of modern warfare – circa 19th century – and Cognitive Warfare would be conceived of as a sub-set of political warfare, trickery, destabilization operations, and military strategy. The second age would correspond to the written medium and its broad distribution, along with the fast propagation of information by early electronic communication. This second age would include mobilization and ideologies as characteristics that drive the Cognitive Warfare that is specific to it. Higher basic literacy and exposure to more information play a role as well. The first age would target those with decision-making power, whereas the second age would seem to address the masses as collective bodies with agency and influence.

The third age is about digital means that can reach individuals in a non-public way and describes Cognitive Warfare as a phenomenon targeting individuals in masses and masses being targeted to influence leadership and decision-making.

For both the second and third ages we see references to traditional lines of warfare activities such as information operations, psychological operations, and propaganda; with the advent of digital means, we also see the addition of cyber(security) / cyber-enabled means and digitally induced cognitive-affective effects. Many authors remain tributary to disciplinary and practice roots, thus reflecting more on information and psychological operations than on some form of potential cognitive (security/military) operations – or Cognitive Warfare.

We are witnessing some geographic and cultural particularities as well. The Transatlantic space speaking of Cognitive Warfare appears bound by the history of cyber and psychological warfare. A segment of Central-Eastern European authors and former Soviet area of influence origin are tying Cognitive Warfare to high level strategy, [26] describing it as an element central to thinking about war strategy. Finally, there appears to be a Chinese conceptualization[7], derived from early Soviet and Cold War thought, infused with ideology, ethno-centrism, decolonization, post-colonial struggle, etc.

[4] Publications were chosen in a first instance based on recency and focus on Cognitive Warfare in an attempt to draw on other authors' investigations into the origins and lineages of how we have reached the concept of "Cognitive Warfare" in the period 2020-2023; in contrast to publications from the 1990s-2010s, which would talk primarily about "cognitive operations" or hybrid warfare. Then the body of literature was expanded to investigate earlier authors' writings about specific aspects of Cognitive Warfare.

[5] Drawing primarily upon Spildsboel Hansen 2021 [23], Cowles & Verrall 2023 [24], Hung & Hung 2020 [25], Maksymenko & Derkach 2023 [26].

[6] Maksymenko & Derkach 2023 [26], p. 132, develop a periodization of military strategies in three stages: Classical (Sun Tzu to the 19th century), Evolutionary theories (19th-20th centuries), and Contemporary theories of psychological warfare (21st century). Drawing upon this example but considering from the perspective of developmental stages of Cognitive Warfare in its contemporary understanding, we determine a four-stage evolution, which also largely corresponds to the ages of scientific and technological development (paper written communication, the printing press / mass production, the telegraph and fast distribution of printed materials, digital means of communication / permanent access), and is correlated also with the degree and ease of access with which adversaries can reach populations, thus starting at the level of small but quasi-isolated communities in between which information could take years to reach, to contemporary times in which information and access are pervasive, persistent, and the environment can even be pre-set-up or continuously shaped for priming target populations.

[7] Note: For the purposes of this review we have examined literature on Chinese Cognitive Warfare. However, rather than country specific, in the broader phenomenon of influence operations, hybrid and Cognitive Warfare thought, this would be

The fourth age of Cognitive Warfare is currently under way, with a distinct emphasis of trying to understand the phenomenon wholistically and not path- or domain-dependent. It makes use of concepts and operations from information, influence, and psychological warfare, cyber means (both as a vehicle and as an attack vector) [24], with several authors including observations about the re-emergence of political warfare, particularly after the financial crash of 2008 (by China), and after 2014 (the first invasion of Ukraine by Russia). The most distinct aspect is the intense focus on neuroscience, behavioral science, and psychology, and the intersection of these sciences with the human functioning at its core. While previous ages focused on things that humans were doing, this last age examined first and foremost how humans' function individually, then collectively, and then what and how they are doing. Thus, we see an increasing number of authors examining the inter-relations between these disciplines (see the chronological list on pages 7-8 in [24]) and how scientific and technological advancements are increasingly allowing their weaponization in the context of warfare.

Epistemologically, the majority of the of the scientific knowledge mobilized towards describing Cognitive Warfare falls under the following domain clusters:

- Cognitive, behavioral, and psychological sciences – to explain the initiation (planning) of campaigns as well as why Cognitive Warfare (and its adjacent warfares) works.
- Operational (military) art, communication sciences, and digital (cyber) vectors – to explain the targeting and conduct of the campaigns.
- Sociology, psychology, ideology, and political sciences to explain the effects.

There appears to be no academic work that describes and analyses examples of demonstrated causality constructs. Many examples are rationalizations of empirical observations that fit a reconceptualized model of Cognitive Warfare. At least, the explanations appear insufficient, particularly considering the recent increased focus on the cognitive, behavioral, psychological sciences, whereas analysis continues to focus substantially on disinformation campaigns, (geo-) politics, cybersecurity and digital channels, etc.

3.2 Definitions of Cognitive Warfare

In 2022, NATO Allied Command Transformation (ACT) proposed a working draft definition of Cognitive Warfare: "Activities conducted in synchronization with other Instruments of Power to affect attitudes and behavior by influencing, protecting, or disrupting individual and group cognition to gain advantage over an adversary" ([14], p. 3), pointing out that "these effects (of Cognitive Warfare) occur within an individual (intra-personal) as well as between people (inter-personal) [24].

Based on the inventory by Cowles and Verrall [24] we can derive the following categorization of Cognitive Warfare:

- **By instrumentalization:** subversion (Rosner & Siman-Tov 2018 [27], Backes & Swab 2019 [4]), dissonance (Pocheptsov 2018 [28], Silverstein 2019 [29]), bias (inducing), vulnerabilities, manipulation, dominance (Maksymenko & Derkach 2023 [26], Hung & Hung 2020 [25]), health, cost, control (Bernal et al. 2020 [30], Beauchamp-Mustafaga 2023 [31], Hung & Hung 2020 [25], Yu & Ho 2022 [32]), capability, liberty, enhancement, barriers, harm, capabilities, quality, capabilities, integrity, (personal) resilience.

better described as a post-colonial view, with a broad spread across the Global South; these views existed pre-2008 – thus before any meaningful Chinese ramp-up of media operations across the Global South, and converged on an agreement about the meaning of influencing and Cognitive Warfare before China routinely started posting media content using the notion of "Western Cognitive Warfare" as of the beginning of Covid-19; however, me may consider that the gradual increase in tensions during the period 2016-2020 would have primed populations towards a higher degree of receptivity once the Covid-19 pandemic started.

- **By locus:** personal, inter-personal, meta-cognitive (NATO ACT exploratory concept [14]), psychological, cognition, behavioral, operations, functional/institutional (skills), battleground (Leucea 2022 [33], dit Avocat 2021 [34], Eshrat-abadi & Moghani 2022 [35], Kania & Wood 2021 [36]).
- **By threat:** security (personal and supra-personal), modelling (shaping), compromising (accessing, influencing), perception, risk (aversion/appetite) (Hung & Hung 2020 [25]), resilience (capacity to exercise judgement, delivering the job), (cognitive) loop (Paul Groestad at CyCon 2022 [19]).
- **By engagement:** attacks, subversion (Rosner & Siman-Tov 2018 [27]), infiltration (Hung & Hung 2020 [25]), combat, impacts, enhancement (Rice & Selman, 2022 [37]), (cognitive) loop (Paul Groestad at CyCon 2022 [19]), defence.

The predominant interpretations of cognition cluster around cognition as the ability to reason and, in an operational capacity, as the ability and/or willingness to conduct war, defence, and carrying out orders.

Reflexive conditioning and contextually or environmentally triggered or induced degradation of cognition – though this is found in academic literature as shaping the environment for inducing indirect effects, particularly around perception of reality and orientation in decision-making – are not discussed as degradation, in a military or biological sense, but rather as 'influencing the mind, perception, and decision-making.

We observe a clustering of types primarily into two broad domains: the biological, centered on cognition, and described as "the micro-level of intra-brain processes and functioning via brain science and cognitive neuroscience" [24] and the security and strategic intelligence realm, drawing on the subversive and covert nature of intelligence work (or "intercultural competence" for Russia [23]), but without encompassing the totality of intelligence approaches to behavior and cognition.

NATO ACT's Concept and the DSTL Report bring a new lens on Cognitive Warfare, focusing on the behavioral-cognitive-psychological perspectives, whereas the majority of the academic authors remain tributary to lineages of hybrid warfare for notions such as indirect effects and the leveraging, or weaponization of societal, cultural, and values-ethical dimensions, rather than being considered part of the Cognitive Warfare toolbox as tactics, techniques, and procedures.

Some of the observable outcomes of Cognitive Warfare are similar to soft power effects[8], bypassing entirely the need for the use of sharp power – which would antagonize populations and alert the security ecosystem [25]. If Cognitive Warfare can deliver similar effects and outcomes to soft and sharp power without the drawbacks, this would constitute an evolutionary step from hybrid warfare, which has the drawback of visibility of TTPs (most of the times).

Siteanu [39] brings a distinct view by highlighting the moving away from Clausewitzian war – the signaling of shift in paradigm is significant. Both him and Vaduva [40] emphasize the aim of achieving epistemological dominance – a notion that we only find again 15 years later in the ACT Concept.

Cognitive warfare is a strategy for altering thinking ([4], p. 8), weaponizing public opinion ([30], p. 3), manipulating environmental stimuli ([6], p. 1). It is also a technological element – as driver, vehicle, and vector ([34], p. 62). Finally, it is a "convergence of "Cyber-Psychology," "Weaponization of Neurosciences," and "Cyber-Influence" for perception alteration ([41], p. 14).

[8] Cowles & Verrall [24], p. 9, reference the recognized activities that fall under soft power: UK MOD (2015) Joint Doctrine Note 1/15 on Defence Engagement https://www.gov.uk/government/publications/defence-engagement-jdn-115); Hung & Hung [25] p.11; Winnerstig [38].

Landes in: [24] sees it as a weapon of the weak in an asymmetrical conflict – an outlier and contrasting opinion, as other authors describe high levels of capabilities mobilized towards Cognitive Warfare – meaning currently it is mostly a battlefield of the strong. And while stemming from traditional kinetic warfare, Miller [42] talks about Cognitive Warfare as if also an evolution beyond kinetic warfare. He considers it a covert means to target the whole population with the purpose of changing its way of thinking ([42], p. 46).

Backes & Swab's [4] perspective opens maximally the spectrum of the content and means of delivery to anything that can be considered information, including things like art, various types of literatures, the virtual world, anything that can be analyzed by semiotics as conveying a message, etc. This corroborates with Hung & Hung [25], Yu & Ho [32], who also write about the influence through culture, resulting a convergent perspective that while Western authors focus on the technologies enabling Cognitive Warfare, there may be a convergence of thought between Russia and China on the usage of culture, values, symbols, to influence. This convergence is further substantiated by the topics they target, focusing on democratic weaknesses, the misinterpretation of Western actions, etc.

Their conceptualization of any information altering actions automatically putting parties in an adversarial position would imply that target governments would treat the situation as hostile. This draws near to the ACT's concept, which proposes that such activities are a "violation of sovereignty and a breach of international law" ([14], p. 13). Danyk & Briggs also take the view that everyone in society is targeted, even at peace ([43], p. 35). Due to its indiscriminate nature and definitional use of society for indirect effects, Cognitive Warfare can be determined to be permanently illegal under international humanitarian law ([14], p. 13). The only exception would be, per the Concept, if Cognitive Warfare was directed exclusively at military leadership. However, this level of precision targeting would stand in contrast with all the other conceptualization of Cognitive Warfare.

Hung & Hung's [25] wording strongly denotes an element of command and control ("controlling others' mental states and behaviors"), drawing on Bernal et al. [30] ("Cognitive Warfare aims to control the responses of individuals and groups to the presented information"), which constitutes a departure from the common understanding that the purpose in hybrid and Cognitive Warfare is to trigger behaviors and influence choices, rather than control actions. They ground their perspective on Cognitive Warfare on the notion that it is a subset of psychological operation and information warfare [44], as well as of Russia's information and cyber-warfare [45], [46], [47], but don't go deeper in Rosner and Siman-Tov's [27] intersection between propaganda, public relations, and public diplomacy as methods for Cognitive Warfare. Similarly, dit Advocat [34] also seems to draw on marketing and public relations concepts, explaining that Cognitive Warfare aims to engage both the brain's system 1 (nudging) and system 2 (coercion).

In relation to the notion of control we have that of coordination and synchronicity of activities, which ACT and DSTL supports, and which for Yu & Ho [32] are a key feature of Cognitive Warfare.

Silverstein [29] focuses on the sub-personal level, focusing on the neuroscientific aspects, while Pocheptsov [28] describes the modularity and combinatorics possibilities of Cognitive Warfare. Considered together, this describes a novel understanding of Cognitive Warfare, in contrast with other non-kinetic warfares: the versatility and unlimited possibilities of layers and combining Cognitive Warfare with any number and other types of activities.

At the supra-personal level, Maksymenko & Derkach [26] propose that Cognitive Warfare relies on social engineering and neuroscience.

At the other end of the spectrum, describing a very technology-intensive mode of Cognitive Warfare, Burke et al. [48] describe Beijing's concept of "information dominance, where big data and artificial intelligence (AI) play important roles in winning the war," introducing a new dimension of automation in and artificially

generated content – a further step beyond the technologies we have seen with social media. Yu & Ho may provide a hint as to the origins of the Chinese concept, dating back to their 2014 "brain control" ([32], p. 252). ACT's Concept goes even further to propose that electromagnetic warfare would also have a role in Cognitive Warfare; but remains an outlier, as academic literature does not approach this side of the spectrum.

Aggregating the views of the various authors, we see that Cognitive Warfare is believed to operate at every single personal and social/societal level, operating insidiously at conscious and unconscious level, with effects ranging from mere inoculation of doubt ([41], pp. 1-5) to outright control over actions that can lead to governmental and constitutional order collapse, and with a potential for automation and scalability derived from the latest technological developments.

The smallest commonly accepted and prevalent conceptualization is that Cognitive Warfare is a battle for the human mind with the purpose of changing decision-making ([33], p. 78), ([49], pp. 1-4).

3.3 What's Missing in Cognitive Warfare Literature: Remaining Research Gaps

Several aspects are only marginally touched upon and insufficiently treated yet in the reviewed academic literature. Health and its weaponization in Cognitive Warfare is mentioned by Yu & Ho [32] in relation to China in the context of Covid 19, but bio-pharmacologically induced alterations to cognition are not yet discussed, which would be the biological sciences equivalent of discussing electromagnetic warfare for those coming from a cyber and technological disciplinary perspective. While Beauchamp-Mustafaga [31] writes extensively about the various Chinese theoretical explorations in circa the mid-2010s about future warfare at the intersection of the biological and technological, drawing heavily on the neurosciences and brain alteration, Western sources do not appear to draw on similar interests and sources, resulting in an almost absence of writings on such approaches – which may, even, be illegal in the transatlantic space.

Another under-discussed dimension deals with ethical challenges such as cultural shaping and values-based attacks and attacks on values, which could be described as the practice of undermining cognition by weaponizing existing cultures and values into personal cognitive dissonances or orchestrating clashes and tensions which cannot be arbitraged objectively, both culture and values being protected spheres, not least by international law. At the same time, this is a missed opportunity at connecting ethics and legal studies with psychological-behavioral dimensions of Cognitive Warfare, and how a mesh of legal structures protecting culture and the biological existence of the individual could be mobilized towards increased protection from Cognitive Warfare. NATO ACT's Concept is the publication that goes furthest discussing possible options for addressing Cognitive Warfare. However, it seems that it remains tributary to an over-emphasis on resilience building via digital literacy, debunking, informing, etc. – the activities typically prescribed in information and hybrid warfare for whole-of-government actions, resulting in an uneven proportion allocated to potential remedies about which much was already written and missing the opportunity to spearhead discussions about features of Cognitive Warfare which are not so prevalent in the public examination.

Cowles & Verrall [24] are listing fields of application of Cognitive Warfare (military, international relations, political science, security, and war studies). This list could be further broken down into direct application by practice (operations) and the theoretical disciplines which inform our world view, concepts, norms, and the ordering principles of our societies. While this latter sub-grouping appears to be implicitly stated by the authors, it would warrant a distinct consideration by academic scholarship, as distinguishing a direct causality between altered cognition and the thinking behind the functioning of our societies would describe the possibility of Cognitive Warfare producing systemic, structural, and mass impairment and degradation of governability (the thinking behind the act of governing), governance, and the operational continuity of governance in a given territory. The academic demonstrability of the causation linkages between all these elements would help consecrate Cognitive Warfare from an academic perspective as a valid interdisciplinary concept.

While these linkages are talked about routinely in hybrid warfare, the theoretical-academic links are frail and based on social sciences hypotheses which only for the past few years have started being confronted with experiments from the neuro-, cognitive-, and behavioral sciences, with the result that sometimes firm hypotheses from the social sciences that explained why disinformation works, for example, have been moderated by in-depth studies that demonstrated only minimal impacts or causality.

Uniquely regarding Chinese conceptualizations on Cognitive Warfare, Beauchamp-Mustafaga [31] describes the People's Liberation Army (PLA) intended capability of predicting decision-making outcomes based on Cognitive Warfare inputs (operations) by mobilizing technological means (for the modelling of the effects). Based on developments in sensors, machine learning and other forms of technology broadly known as 'artificial intelligence', behavior modelling appears to have become possible, but it remains unclear whether this can be achieved for a mass of people. Implied but not explicit across the literature is the notion that, for the purpose of collapsing a country's governability, Cognitive Warfare may be sufficient, in lieu of kinetic engagement, with the added advantages of being covert, hard to detect, and can be operated with lower costs. While most authors focus on applications in defence and security, a few mention the corporate realm as enablers (e.g., disinformation propagated via social media), but none mention corporate leaders' decision making and how their actions may influence the outcomes of war (e.g., Elon Musk and the role of the SpaceX service Starlink in the war in Ukraine). As an attack surface, the private sector population represents the highest risk[9], being over-represented, over-exposed, and under-trained to be resilient or at least aware when faced with the peculiarities of Cognitive Warfare.

Hung & Hung provide an account of the fact that many authors and academic scholarship concern themselves with inputs and throughputs – what goes into Cognitive Warfare and how these inputs are processed cognitively, but the research appears to be thinner on the analysis of affective treatment of inputs, as well as on the effects – thus highlighting an uncertainty in correlation, or the demonstration of causality ([25], pp. 3-4). They further highlight the lack of critical assessment of the proposed models, and even possibly a failure to adequately mobilize knowledge from the cognitive sciences for the examination of Cognitive Warfare.

4.0 RELATION TO NEIGHBORING CONCEPTS

4.1 Key Questions

The focus of our paper is the analysis of the concept Cognitive Warfare. However, two other concepts are seemingly closely conceptually related to Cognitive Warfare: Hybrid Threats as well as Foreign Information Manipulation and Interference (FIMI). The following section will explore the questions of whether an overlap exists in the literature surrounding the three concepts, whether there is interoperability between the concepts, and whether, if so, a conceptual overlap can be identified. These questions would each be the subject of a separate investigation, so only an initial attempt to map the conceptual terrain can be made below.[10]

4.2 Basic Comparison

First, before any more profound analysis of the conceptual dimension, the question arises as to why the three concepts of Cognitive Warfare, Hybrid Threats, and FIMI exist in parallel.

[9] Yu & Ho ([32], p. 250), describe situations in which companies across the world were affected during the covid pandemic by Chinese claimed Cognitive Warfare, thus demonstrating the economic security implications that know no national boundaries.

[10] For an investigation of the role of disinformation tactics in the concepts Cognitive Warfare, Hybrid Threats and FIMI see [50].

In the scientific domain, one would assume that each concept must be sufficiently distinct and serve a specific epistemic interest to have a right to exist and be used in academic research. However, Cognitive Warfare, Hybrid Threats, and FIMI are not primarily in the academic domain.

Therefore, to identify and explain the coexistence of the three concepts as well as the conceptual overlaps, it is necessary to make three points: First, the three concepts emerged at different times. The oldest concept is Hybrid Threats, followed by Cognitive Warfare (as a concept). The most recent concept is FIMI. Therefore, aggregate concept development is to be expected.

Second, the three concepts were developed by different institutions and in different domains. The FIMI concept was primarily created by the EU, more specifically, the European External Action Service (EEAS). While academically inspired, Hybrid Threats has been significantly developed within Europe by the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE). Cognitive Warfare came into discussion and was introduced primarily through NATO, some members of the alliance and related institutions.

The three concepts are thus in different domains [50], tending to be the military, the policy, and the academic spheres. Each of these spheres operates according to its own logic. Against this background, it is expected that interchange between the spheres and conceptual borrowing will be slower than if all three concepts are located in the same sphere, especially the academic sphere.

Finally, while the three concepts target similar threat situations, they target different responses:

1) Cognitive Warfare conceptualizes a threat to Military Instruments of Power, with potentially large scale whole-of-society implications and effects, that is located below the threshold of armed conflict ([14], p. 5). However, on the continuum of competition, confrontations which are already past the realm of the rule-based international order can potentially grow into kinetic conflicts ([51], p. 5 ff.). In the 2022 NATO Madrid Summit Declaration, Cognitive Warfare is not explicitly mentioned, however many tactics which are conceptualized to be part of Cognitive Warfare are mentioned. The declaration states “cyber, space, and hybrid and other asymmetric threats, and (…) the malicious use of emerging and disruptive technologies” [52] need to be addressed with integrated responses that include, among many others, the national building of resilience to cyber and hybrid threats.
2) Hybrid Threats, as conceptualized by Hybrid CoE may be mitigated using a whole-of-society approach that focuses on establishing a Comprehensive Resilience Ecosystem (CORE) in democratic societies [53].
3) EEAS definiens Foreign Information Manipulation and Interference (FIMI) as “a mostly non-illegal pattern of behavior that threatens or has the potential to negatively impact values, procedures, and political processes. Such activity is manipulative, intentional, and coordinated for effect. Actors of such activity can be state or non-state actors, including their proxies inside and outside of their own territory” ([22], p. 25). The EEAS envisions a comprehensive strategy to mitigate the impact of FIMI on democratic institutions and societies. This approach encompasses strengthening situational awareness, developing tailored policies and strategies for response, providing strategic communications support to EU delegations and CSDP missions, enhancing public resilience and awareness, fortifying neighboring countries’ capacity, and fostering cooperation with international partners. This multifaceted strategy aims to create a robust defense against the challenges posed by FIMI, both on the EU and national levels [22].

Resilience of societies, institutions and individuals plays a central role in all three concepts to respond to and mitigate the identified vulnerabilities. Nonetheless, these concepts are distinctly oriented toward various societal domains and institutions. Therefore, the approaches to enhancing resilience and the key institutions and processes involved vary significantly.

4.3 Methodology

The initial overview revealed that the three concepts were crafted within specific domains with distinct objectives. However, a deeper exploration is needed to understand the extent of interoperability or potential conceptual overlap. Given that this section is meant to provide only a rough orientation regarding the neighboring concepts, a full-scale concept analysis of all three concepts will be omitted. Instead, an alternative approach utilizing a large language model is employed to identify conceptual overlaps. This involves a semantic analysis of the three concepts. Methodologically, we pinpointed reference papers in which the concepts were currently and authoritatively elaborated. These papers represent pivotal institutions and influential actors in developing these concepts.

For the Cognitive Warfare concept the main reference document is the explanatory concept by NATO ACT along with further relevant publications [14]. In the exploratory concept by NATO ACT, Cognitive Warfare is defined as follows: “Activities conducted in synchronization with other Instruments of Power, to affect attitudes and behavior by influencing, protecting, or disrupting individual and group cognition to gain advantage over an adversary” ([14], p. 3).

The main reference document for Hybrid Threats is “Hybrid Threats - A comprehensive resilience ecosystem” by the Hybrid CoE [53]. In the reference document Hybrid Threats are defined as follows: “Hybrid threats constitute a combination of different types of tools, some expected and known, some unexpected and clandestine, applied to achieve an undeclared strategic objective, and without officially admitting to doing so. The common denominator for hybrid threat actors is their desire to undermine or harm democratically established governments, countries or alliances” ([53], p. 8). The goal of the tactics mentioned above is conceptualized to “manipulate established decision-making processes by blurring situational awareness, exploiting gaps in information flows, intimidating individuals and creating fear factors in target societies” ([53], p. 8).

For Foreign Information Manipulation and Interference the reference documents are the most recent reports by EEAS [22], [54], [55]. The definition of Foreign Information Manipulation and Interference by EEAS is:

> *Foreign Information Manipulation and Interference (FIMI) describes a mostly non-illegal pattern of behavior that threatens or has the potential to negatively impact values, procedures and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner, by state or non-state actors, including their proxies inside and outside of their own territory* ([22], p. 4).

EEAS sees the whole-of-society approach crucial to successfully counter the effects of FIMI: “The whole-of-society approach is a key element in the EEAS’ work to prevent, deter and respond to FIMI” ([22], p. 7).

After identifying the core conceptual documents, we used a Large Language Model Service, namely the app Lateral (https://app.lateral.io). Lateral allows, within a self-created text-corpus, to annotate concepts through manual annotations (Similar to ATLAS Ti or MaxQDATA). Given a sufficiently large training data set, the program can search for the concept’s content in other papers using semantic analysis. Following the grounded theory approach, we iteratively identified the concepts as we worked through each reference document multiple times. We manually annotated the concepts “Hybrid Threats,” “Foreign Information Manipulation and Interference (FIMI)” and “Cognitive Warfare” in Lateral. The training dataset was sufficiently large (n>100) for Lateral to independently find additional suggestions for identical concepts with modified semantics in the text corpus using semantic analysis.

Following the manual annotation of the concepts, we searched for each of the three concepts in the base documents of the other two concepts, using the semantic tools provided by Lateral for concept search.

4.4 Results

The cross-check of these concepts, conducted at a broader semantic level rather than an academically nuanced terminology level, yielded intriguing results. Specifically, Cognitive Warfare, hybrid threats, and FIMI demonstrated a high degree of interchangeability in semantic searches. This interchangeability primarily pertains to FIMI and Hybrid Threats, with a secondary level of conceptual proximity to Cognitive Warfare. In the recent conceptual specification of Hybrid Threats through CORE by the Hybrid COE, substantial overlap with the concept of FIMI was observed. Additionally, the cross-dimensional attack sectors specified in the concept of Cognitive Warfare displayed significant proximities to both Hybrid Threats and FIMI.

However, in the realm of resilience conceptualization, the semantic search in Lateral revealed less overlap. Here, distinct conceptual differences were identified between Cognitive Warfare on one hand, and Hybrid Threats and FIMI on the other. The latter two concepts incorporate a whole-of-society approach, varying in depth. This difference arises due to specific domain-related and political considerations in NATO's foundational documents on Cognitive Warfare. Based on this semantic concept analysis, there is a notable level of interoperability among the three concepts. Noteworthy distinctions do emerge, particularly in the realm of resilience enhancement against these vulnerabilities.

5.0 CONCLUSION

The purpose of this paper was to gain a better understanding of the concept of Cognitive Warfare. Hereby, the work was aimed at answering the three research questions. The first research question was: Does the Cognitive Warfare Concept by NATO ACT offer analytical capacities from a political science standpoint, or is its primary utility confined to institutional military applications?

The Cognitive Warfare Concept, as published in the Exploratory Concept by NATO ACT [14], represents a comprehensive conceptualization of novel forms of conflict and competition in the contemporary global security landscape. Defined as Activities conducted in synchronization with other Instruments of Power, to affect attitudes and behavior by influencing, protecting, or disrupting individual and group cognition to gain advantage over an adversary" ([14], p. 3) Cognitive Warfare operates within the Information Environment using Emerging Disruptive Technologies (EDTs) to target individuals, groups, or societies vulnerable to cognitive attacks. The concept is characterized by its focus on the manipulation of emotional and subconscious processes, thus distinguishing it from related concepts like Hybrid Threats and Foreign Information Manipulation and Interference (FIMI). It addresses the evolving challenges posed by technological progress, shifts in the information environment, and the leveraging of societal divisions. The methodological evaluation of the military concept reveals several shortcomings, which make it difficult to use the concept for empirical research, for example operationalization presents challenges due to the lack of concrete instances in the field and the covert nature of associated tactics. The concept's validity is contingent on future developments, as its forward-looking nature aligns with emerging threats. While currently facing some limitations in empirical research, Cognitive Warfare holds significant analytical potential in contexts focused on emerging threats.

In summary, the Cognitive Warfare Concept offers valuable analytical capacities from a political science standpoint, providing a framework to comprehend and address the complex challenges presented by cognitive attacks in the contemporary global security environment. While it requires further refinement and empirical validation, it can potentially be a valuable tool for understanding and mitigating informational attacks through emerging technologies on decision-making processes, societal cohesion, and the overall security landscape.

Research question 2 is: How is Cognitive Warfare conceptualized and represented in scientific literature?

Cognitive Warfare, as conceptualized and represented in scientific literature, has evolved through distinct phases of conceptualization. These phases can be broadly categorized into four ages. The first age, which traces back to ancient strategists like Sun Tzu, extends until the 19th century. During this period, Cognitive Warfare was seen as a subset of political warfare, encompassing tactics like trickery, destabilization operations, and military strategy. The second age emerged with the proliferation of written communication and early electronic means of information dissemination. This era introduced mobilization and ideologies as key drivers of Cognitive Warfare, with a focus on influencing the masses collectively. The third age centers around digital means, targeting individuals on a non-public level. It characterizes Cognitive Warfare as a phenomenon aimed at influencing leadership and decision-making through mass targeting. The fourth age, the current phase, emphasizes a holistic understanding of Cognitive Warfare, transcending specific domains or pathways. It incorporates concepts and operations from information, influence, and psychological warfare, along with the integration of cyber capabilities. Notably, this age places a strong emphasis on neuroscience, behavioral science, and psychology, examining how these sciences intersect with human functioning. In examining the literature, several domains of scientific knowledge contribute to the understanding of Cognitive Warfare:

1) **Cognitive, Behavioral, and Psychological Sciences:** These domains are essential for explaining the initiation and planning of Cognitive Warfare campaigns, as well as understanding why Cognitive Warfare is effective.
2) **Operational (Military) Art, Communication Sciences, and Digital (Cyber) Vectors:** These areas elucidate the targeting and execution of Cognitive Warfare campaigns.
3) **Sociology, Psychology, Ideology, and Political Sciences:** These fields help explain the effects of Cognitive Warfare.

Despite a growing number of publications on Cognitive Warfare, there is a notable absence of academic work that provides concrete examples of demonstrated causality constructs. Many examples seem to be rationalizations of empirical observations rather than rigorous causal analyses. Additionally, the literature tends to focus on areas like disinformation campaigns, geopolitics, and digital channels, often overlooking the deeper psychological and behavioral aspects. In terms of definitions, NATO Allied Command Transformation (ACT) proposed a working draft definition of Cognitive Warfare in 2023. It characterizes Cognitive Warfare as activities conducted in sync with other Instruments of Power to influence, protect, or disrupt individual and group cognition, aiming to gain an advantage over an adversary. This definition emphasizes that Cognitive Warfare affects both intra-personal and inter-personal levels. Cognitive warfare can be further categorized based on instrumentalization, locus, threat, and engagement, offering a comprehensive framework for understanding its multifaceted nature. Notably, Cognitive Warfare operates at various levels, from personal to societal, and employs a wide range of strategies and tactics, including psychological operations, information warfare, and social engineering. Overall, the literature highlights the complexity and dynamism of Cognitive Warfare, emphasizing the need for a multidisciplinary approach that encompasses psychological, behavioral, and technological dimensions. The evolving nature of Cognitive Warfare necessitates continuous research and analysis to stay ahead of emerging threats and strategies.

Research question 3 is: What are the functional and analytical disparities in comparison to neighboring concepts, namely FIMI and Hybrid Threats and how are the three concepts related?

The coexistence of these three concepts can be attributed to their distinct origins and purposes. Hybrid Threats emerged earliest, followed by Cognitive Warfare, with FIMI being the most recent addition to this conceptual landscape. These concepts were developed by different institutions in separate domains - Hybrid Threats by the European Centre of Excellence for Countering Hybrid Threats, Cognitive Warfare primarily through NATO, and FIMI by the European External Action Service. Each concept operates within its own

sphere, be it military, political, or academic. This compartmentalization can slow down the exchange of ideas and the adoption of concepts across these domains. In terms of response, Cognitive Warfare primarily concerns threats to Military Instruments of Power below the threshold of armed conflict. Hybrid Threats, as defined by Hybrid CoE, can be countered through a Comprehensive Resilience Ecosystem (CORE) in democratic societies. FIMI, defined by EEAS, focuses on countering manipulative behavior that threatens democratic values, procedures, and political processes. In their core documents, there is substantial terminological overlap, especially between FIMI and Hybrid Threats. Additionally, Cognitive Warfare demonstrates a certain degree of semantic proximity to both Hybrid Threats and FIMI. However, when it comes to resilience enhancement, there are discernible differences. Cognitive Warfare places a distinct emphasis on Military Instruments of Power. Hybrid Threats and FIMI, on the other hand, adopt a whole-of-society approach, albeit with varying depths.

To summarize, while these concepts share similarities in targeting specific threat scenarios and advocating for resilience, they also possess unique attributes stemming from their institutional origins and distinct focus areas. This diversity reflects the varied responses required to address the multifaceted challenges posed by modern threats.

6.0 BIBLIOGRAPHY

[1] B. Claverie and F. du Cluzel, "The Cognitive Warfare Concept," NATO ACT Innovation Hub, 2021. [Online]. Available: https://www.innovationhub-act.org/sites/default/files/2022-02/CW%20article%20Claverie%20du%20Cluzel%20final_0.pdf

[2] F. du Cluzel, "Cognitive Warfare," NATO ACT Innovation Hub, 2021. [Online]. Available: https://www.innovationhub-act.org/sites/default/files/2021-01/20210122_CW%20Final.pdf

[3] D. F. Reding and B. Wells, "Cognitive Warfare: NATO, COVID-19 and the Impact of Emerging and Disruptive Technologies," in COVID-19 Disinformation: A Multi-National, Whole of Society Perspective, R. Gill and R. Goolsby, Eds., in Advanced Sciences and Technologies for Security Applications., Cham: Springer International Publishing, 2022, pp. 25–45. doi: 10.1007/978-3-030-94825-2_2.

[4] O. Backes and A. Swab, "Cognitive Warfare: The Russian Threat to Election Integrity in the Baltic States," Harvard Kenney School Belfer Center for Science and International Affairs, 2019. Accessed: Feb. 03, 2023. [Online]. Available: https://www.belfercenter.org/publication/cognitive-warfare-russian-threat-election-integrity-baltic-states

[5] F. Splidsboel Hansen, "When Russia Wages War in the Cognitive Domain," The Journal of Slavic Military Studies, vol. 34, no. 2, pp. 181–201, Apr. 2021, doi: 10.1080/13518046.2021.1990562.

[6] T.-C. Hung and T.-W. Hung, "How China's Cognitive Warfare Works: A Frontline Perspective of Taiwan's Anti-Disinformation Wars," Journal of Global Security Studies, vol. 7, no. 4, p. ogac016, Dec. 2022, doi: 10.1093/jogss/ogac016.

[7] S. Schieder, "Institutionalismus in den Internationalen Beziehungen," in Handbuch Internationale Beziehungen, C. Masala and F. Sauer, Eds., in Springer NachschlageWissen. , Wiesbaden: VS Verlag für Sozialwissenschaften, 2015, pp. 1–31. doi: 10.1007/978-3-531-19954-2_6-1.

[8] G. Sartori, "Concept Misformation in Comparative Politics," Am Polit Sci Rev, vol. 64, no. 4, pp. 1033–1053, 1970, doi: 10.2307/1958356.

[9] J. Gerring, Ed., "Concepts," in Social Science Methodology: A Criterial Framework, Cambridge: Cambridge University Press, 2001, pp. 33–64. Accessed: Oct. 28, 2023. [Online]. Available: https://www.cambridge.org/core/books/social-science-methodology/concepts/E152BE9B504B9DFD91321DD3FF777A81

[10] NATO Allied Command Transformation (ACT), "Concept Development and Experimentation Handbook," NATO Allied Command Transformation (ACT), Norfolk, VA, Version 2.10, Aug. 2021. [Online]. Available: https://www.act.nato.int/wp-content/uploads/2023/05/NATO-ACT-CDE-Handbook_A_Concept_Developers_Toolbox.pdf

[11] D. Collier and J. E. Mahon, "Conceptual 'Stretching' Revisited: Adapting Categories in Comparative Analysis," The American Political Science Review, vol. 87, no. 4, pp. 845–855, 1993, doi: 10.2307/2938818.

[12] V. A. Schmidt, "Discursive Institutionalism: The Explanatory Power of Ideas and Discourse," Annual Review of Political Science, vol. 11, no. 1, pp. 303–326, 2008, doi: 10.1146/annurev.polisci.11.060606.135342

[13] V. A. Schmidt, "Taking ideas and discourse seriously: explaining change through discursive institutionalism as the fourth 'new institutionalism,'" European Political Science Review, vol. 2, no. 1, pp. 1–25, Mar. 2010, doi: 10.1017/S175577390999021X.

[14] NATO Allied Command Transformation (ACT), "Cognitive Warfare Exploratory Concept," NATO Allied Command Transformation (ACT), ACT/SPP/CNDV/TT-6700, Apr. 2023.

[15] R. S. Mueller, "Report on the Investigation into Russian Interference in the 2016 Presidential Election," U.S. Department of Justice, Washington D.C., 2019.

[16] NATO, "NATO 2022 Strategic Concept." Jun. 29, 2022. [Online]. Available: https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf

[17] NATO, "The North Atlantic Treaty." Apr. 04, 1949. Accessed: Oct. 27, 2023. [Online]. Available: https://www.nato.int/cps/en/natohq/official_texts_17120.htm

[18] NATO, "NATO Warfighting Capstone Concept," NATO ACT, Norfolk, VA, 2021. Accessed: Aug. 23, 2023. [Online]. Available: https://www.act.nato.int/our-work/nato-warfighting-capstone-concept/

[19] P. Groestad, "Cognitive Warfare – Hacking the OODA Loop." [Online]. Available: https://www.youtube.com/watch?v=H3RqF5PiqXM

[20] G. Sartori, Ed., Social science concepts: a systematic analysis. Beverly Hills, Calif. [u.a.]: Sage, 1984, p. 455.

[21] C. Wardle and H. Derakhshan, "Information disorder: Toward an interdisciplinary framework for research and policy making," Council of Europe, Strasbourg, 2017. Accessed: Apr. 26, 2021. [Online]. Available: https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html

[22] European Union External Action, "1st EEAS Report on Foreign Information Manipulation and Interference Threats," European Union External Action, Bruxelles, Feb. 2023. [Online]. Available: https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en

[23] F. Splidsboel Hansen, "Russian disinformation - an example." Accessed: Jun. 10, 2021. [Online]. Available: https://www.diis.dk/en/russian-disinformation-an-example

[24] N. Cowles and N. Verrall, "The Cognitive Warfare concept: A short introduction," Defence Science and Technology Laboratory, Salisbury, UK, DSTL/TR146721 v1, 2023.

[25] T.-C. Hung and T.-W. Hung, "How China's Cognitive Warfare Works: A Frontline Perspective of Taiwan's Anti-Disinformation Wars," Journal of Global Security Studies, 2020. doi: 10.1093/jogss/ogac016.

[26] S. D. Maksymenko and L. M. Derkach, "Understanding Modern Cognitive War in The Global Dimension, Its Genesis in The Ukrainian Context: A Review And Directions For Future Research. Cognitive warfare and social impact operations," Defence and Strategy, vol. 23, no. 1, pp. 126–148, Jun. 2023. doi: 10.3849/1802-7199.23.2023.01.126-148.

[27] Y. Rosner and D. Siman-Tov, "Russian Intervention in the US Presidential Elections: The New Threat of Cognitive Subversion," INSS Insight No. 1031 (March), 2018, [Online]. Available: https://www.inss.org.il/publication/russian-intervention-in-the-us-presidential-elections-the-new-threat-of-cognitive-subversion/

[28] G. Pocheptsov, "Cognitive Attacks in Russian Hybrid Warfare," Information & Security, An International Journal, vol. 41, pp. 37–43, 2018.

[29] N. (Naomi) Silverstein, "The New Geopolitical Space in the Information Era: A Neuroscientific Approach to National Security," 2019.

[30] A. Bernal, C. Carter, I. Singh, K. Cao, and O. Madreperla, "Cognitive Warfare - An Attac on Thought and Truth," Johns Hopkins University, Baltimore MD, USA, 2020. [Online]. Available: https://www.innovationhub-act.org/sites/default/files/2021-03/Cognitive%20Warfare.pdf

[31] N. Beauchamp-Mustafaga, "Chinese Next-Generation Psychological Warfare: The Military Applications of Emerging Technologies and Implications for the United States," RAND Corporation, Jun. 2023. Accessed: Oct. 26, 2023. [Online]. Available: https://www.rand.org/pubs/research_reports/RRA853-1.html

[32] M. T.-C. Yu and K. Ho, "COVID and Cognitive Warfare in Taiwan," Journal of Asian and African Studies, vol. 58, no. 2, pp. 249–273, 2022, doi: 10.1177/00219096221137665.

[33] I. Leucea, "The cognitive warfare in designing the international society and the security environment," in Paper presented at the International Conference on Redefining Community in Intercultural Context, Brasov, Romania, May 2022.

[34] A. dit Avocat, "Cognitive Warfare: The Battlefield of Tomorrow?" in New Technologies, Future Conflicts, and Arms Control, Prague: Center for Security Analyses and Prevention, 2021.

[35] H. M. Eshrat-abadi and S. S. Moghani, "Modern Cognitive Warfare: From the Application of Cognitive Science and Technology in the Battlefield to the Arena of Cognitive Warfare," Journal of Human Resource Studies, vol. 12, no. 2, pp. 156–180, 2022, doi: 10.22034/JHRS.2022.158895.

[36] E. Kania and P. Wood, "Sharp Swords of the Future Battlefield: The Chinese Military's Special Forces and Psychological Operations," Strategic Latency Unleashed, vol. 94, pp. 102–15, 2021.

[37] G. Rice and J. Selman, "Sola dosis facit venenum: The Ethics of Soldier Optimisation, Enhancement, and Augmentation," Journal of Military Ethics, vol. 21, no. 2, pp. 97–115, 2022, doi: 10.1080/15027570.2022.2133372.

[38] M. Winnerstig, Ed., Tools of Destabilization: Russian Soft Power and Non-military Influence in the Baltic States. Stockholm: FOI, 2014. [Online]. Available: http://appc.lv/wpcontent/uploads/2014/12/FOI_Non_military.pdf

[39] E. Siteanu, "Knowledge-Based Warfare (Cognitive Warfare)," Strategic Impact, no. 3, 2007, [Online]. Available: https://cssas.unap.ro/en/pdf_periodicals/si24.pdf

[40] G. Vaduva, "Cognitive War?," Strategic Impact, no. 23, 2007.

[41] B. Claverie, B. Prebot, N. Buchler, and F. du Cluzel, "Cognitive Warfare - First NATO scientific meeting on Cognitive Warfare," NATO CSO, Neuilly, France, Jun. 2021. [Online]. Available: https://www.innovationhub-act.org/sites/default/files/2022-03/Cognitive%20Warfare%20Symposium%20-%20ENSC%20-%20March%202022%20Publication.pdf

[42] S. Miller, "Cognitive warfare: an ethical analysis," Ethics Inf Technol, vol. 25, no. 3, p. 46, Sep. 2023, doi: 10.1007/s10676-023-09717-7.

[43] Y. Danyk and C. M. Briggs, "Modern Cognitive Operations and Hybrid Warfare," Journal of Strategic Security, vol. 16, no. 1, pp. 35–50, 2023.

[44] M. C. Libicki, What is Information Warfare? Washington, DC: Institute for National Strategic Studies, National Defence University, 1995.

[45] B. Tashev, M. Purcell, and B. McLaughlin, "Russia's Information Warfare: Exploring the Cognitive Dimension," (U.S.) Marine Corps University Journal, vol. 10, no. 2, pp. 129–147, 2019, doi: 10.21140/mcuj.2019100208.

[46] M. Connell and S. Vogler, "Russia's Approach to Cyber Warfare," CENTER FOR NAVAL ANALYSES ALEXANDRIA VA, ALEXANDRIA United States, Sep. 2016. Accessed: Oct. 26, 2023. [Online]. Available: https://apps.dtic.mil/sti/citations/AD1019062

[47] J. A. Lewis, Cognitive Effect and State Conflict in Cyberspace. Washington, DC: Center for Strategic and International Studies, 2018.

[48] E. J. Burke, K. Gunness, C. A. I. Cooper, and M. Cozad, "People's Liberation Army Operational Concepts," RAND Corporation, Sep. 2020. Accessed: Oct. 27, 2023. [Online]. Available: https://www.rand.org/pubs/research_reports/RRA394-1.html

[49] Y. R. Masakowski and J. M. Blatny, "Mitigating and Responding to Cognitive Warfare: This Technical Report documents the findings of NATO HFM Exploratory Team-356 (PRE-RELEASE VERSION)," NATO STO CSO, Paris, 2022.

[50] C. Deppe, "Disinformation in Cognitive Warfare, Foreign Information Manipulation and Interference, and Hybrid Threats," The Defence Horizon Journal, vol. 2023, Oct. 2023, doi: 10.5281/zenodo.10005172.

[51] NATO, "Nato Standard AJP-01 Allied Joint Doctrine Edition F Version 1." NATO Standardization Office (NSO), Dec. 2022.

[52] NATO, "Madrid Summit Declaration issued by NATO Heads of State and Government (2022)," NATO. Accessed: Oct. 26, 2023. [Online]. Available: https://www.nato.int/cps/en/natohq/official_texts_196951.htm

[53] A. Aho et al., "Hybrid threats: A comprehensive resilience ecosystem," Hybrid CoE - The European Centre of Excellence for Countering Hybrid Threats. Accessed: Oct. 26, 2023. [Online]. Available: https://www.hybridcoe.fi/publications/hybrid-threats-a-comprehensive-resilience-ecosystem/

[54] European Union External Action, "2021 StratCom activity report - Strategic Communication Task Forces and Information Analysis Division," Bruxelles, 2021. Accessed: Aug. 18, 2023. [Online]. Available: https://www.eeas.europa.eu/eeas/2021-stratcom-activity-report-strategic-communication-task-forces-and-information-analysis_en

[55] European Union External Action, "2022 Report on EEAS Activities to Counter FIMI," Feb. 2023. [Online]. Available: https://www.eeas.europa.eu/eeas/2022-report-eeas-activities-counter-fimi_en