Ali Karami [1]

Afshin Mottaghi Dastenaei [2]

The European Union's Approach to Cognitive Warfare's Command and Control

Journal of Electrical Systems

Abstract

Cognitive warfare has evolved alongside advances in technology, psychology, and communication methods, reflecting a growing understanding of how to influence and control human minds. Cognitive warfare refers to efforts to influence, manipulate, or control public perceptions, decision-making processes, and behaviors using psychological, informational, or technological tactics that often blur the lines between the military and civilian domains. From ancient psychological tactics to artificial intelligence-based disinformation campaigns, the essence of cognitive warfare is the same: shaping perceptions and behavior in ways that often achieve strategic goals without the need for physical force. One of the most important aspects of cognitive warfare is its command and control, which naturally has multiple perspectives. This article aims to understand the European Union's approach to command and control of cognitive warfare. The main research question is what similarities and differences does the European Union's approach to command and control of cognitive warfare have with other approaches? The method of this article is descriptive-analytical. The required data was obtained by referring to library sources as well as reputable scientific research articles and official documents. The research findings show that the European Union's approach to command and control in cognitive warfare is shaped by its broader strategy for hybrid threats, cybersecurity, and defense, with a focus on resilience, collective security, and democratic values. The European Union's approach to command and control in cognitive warfare integrates multi-level efforts to protect information integrity, increase public resilience, and promote digital governance while respecting democratic values. Also, in the Union's approach, cooperation with international partners and continuous development of capabilities in command and control of the growing domain of cognitive warfare is crucial.

Keywords: Command and control, hybrid threats, artificial intelligence, media literacy, cognitive interventions.

Cognitive warfare has deep historical roots, although the term itself is relatively modern. Its evolution reflects advances in communication technologies, psychological understanding, and political strategies. Cognitive warfare has been used to influence individuals and populations, targeting emotions, beliefs, and behaviors to gain an advantage in conflicts or competitions (Mottaghi Dastenaei & Karami, 2024). Cognitive warfare has gone through different periods in its evolutionary process:

1- Ancient and Classical Period: Cognitive warfare can be traced back to ancient civilizations such as Greece, Rome, and China. Sun Tzu, a Chinese military strategist (6th century BC), emphasized psychological tactics in his work The Art of War. He recognized the importance of manipulating the enemy's perception of strength and weakness, using deception, disinformation, and psychological pressure to win without war. The Romans used cognitive tactics such as fear-mongering, using myths about their military invincibility, and building monuments to reinforce their power and control over populations. Religious leaders and empires often used rhetoric, symbols, and rituals to manipulate beliefs and perceptions of authority. This set the stage for more systematic cognitive warfare (Miller, 2023).

2- Early Modern Period (16th–18th centuries): The invention of the printing press (1440s) by Johannes Gutenberg revolutionized communication. Governments, religious organizations, and political movements used printing to disseminate information, influence public opinion, and control narratives. The Protestant Reformation (16th century) and the Catholic Counter-Reformation used pamphlets, books, and art as tools to influence public sentiment, shape religious identities, and control the ideological landscape of Europe. At this time in history, Napoleon Bonaparte (early 19th century) was a master of psychological warfare, using proclamations, public displays of power, and disinformation to mentally manipulate his own soldiers and enemy forces (Jones, 2011).

[1] .**Corresponding author :**Alikarami598@ut.ac.ir
[2] .**Email addres:** A.mottaghi@khu.ac.ir
PhD in European Studies, University of Tehran
Full Professor of Political Geography, Kharazmi University

Introduction

3- 19th and early 20th centuries: With the rise of nationalism in the 19th century, we see the increasing use of propaganda by nation-states to unite populations, construct national identities, and demonize enemies. This period also saw the professionalization of public relations and propaganda, especially during wartime. Cognitive warfare took the form of large-scale propaganda efforts during World War I. Nations used posters, radio programs, and newspapers to stir up patriotic fervor, demonize enemies, and influence domestic and foreign populations. The concept of "total war" required the mobilization of civilian populations, making cognitive influence a key aspect of warfare (Editorial Team, 2024).

4- World War II: World War II marked the culmination of state cognitive warfare. The Nazi German Ministry of Information, under the leadership of Joseph Goebbels, turned propaganda into a powerful tool for psychological manipulation, using film, radio, and mass rallies to consolidate power, spread anti-Semitic ideology, and justify military aggression. The Allies, particularly through the British BBC and the United States Office of War Information, used similar techniques to boost morale, demonize the Axis powers, and influence international opinion. Military psychological operations became an official discipline during World War II, aimed at demoralizing enemy soldiers and populations through proclamations, radio broadcasts, and disinformation campaigns (van der Klaauw, 2023).

5- Cold War Era (1947-1991) (The Battle for Hearts and Minds): The Cold War between the United States and the Soviet Union was as much a cognitive war as a geopolitical or military conflict. Both superpowers engaged in extensive psychological warfare, using propaganda, media, cultural exchanges, and covert operations to win the hearts and minds of global populations. The Soviet Union used "active measures," including disinformation campaigns, false narratives, and foreign media influence, to manipulate perceptions in the West and influence global opinion. Conversely, the United States and NATO focused on promoting democratic ideals and undermining communist ideology. The Voice of America and Radio Free Europe broadcast pro-Western messages to communist countries with the aim of creating doubt and inspiring opposition. Cognitive warfare also played a key role in the Vietnam War, particularly through the manipulation of the media and public opinion. The U.S. government's efforts to control the narrative, coupled with the anti-war movement's use of the media to undermine official messages, demonstrated the growing power of cognitive influence in shaping political outcomes (Engerman, 2010).

The EU's approach to cognitive warfare is based on its commitment to democratic principles, human rights, and the rule of law. Command and control strategies must balance the need for security with the protection of fundamental freedoms such as freedom of expression and privacy. The EU General Data Protection Regulation is an example of the EU's efforts to protect citizens' data from misuse in psychological or cognitive operations. From the EU's perspective, cognitive warfare increasingly uses artificial intelligence and machine learning, resulting in the EU's AI strategy including provisions to address the ethical use of AI, particularly in defence and security, and to counter the potential misuse of AI in cognitive manipulation (Europa, 2024). While the EU sets general policies, member states have varying levels of capability and approach in dealing with cognitive warfare. Addressing cognitive warfare requires monitoring of information environments, which raises concerns about privacy, data protection and possible overreach. Cognitive warfare tactics continue to evolve with new technologies, making predicting and defending against emerging threats a constant challenge (Buvarp, 2023). Given this introduction, the aim of this research is to understand the European Union's approach to cognitive warfare command and control. The main research question is what similarities and differences does the European Union's approach to cognitive warfare command and control have with other approaches? The method of this article is descriptive-analytical. The required data was obtained by referring to library sources as well as reputable scientific research articles and official documents.

Theoretical Approach

Cognitive warfare theories focus on the strategic use of psychological, informational, and technological tools to influence, manipulate, or control the cognitive processes of individuals or populations. These theories provide a framework for understanding how human minds, emotions, decision-making processes, and perceptions can be targeted to achieve political, military, or social goals. As technology continues to evolve, particularly in the areas of artificial intelligence, big data, and social media, the application of cognitive warfare theories is likely to become more sophisticated and influential (Ibrahim et al. 2023).

Several academic, military, and psychological theories have been proposed to explain how cognitive warfare works, the most important of which are summarized below:

1- Psychological Warfare Theory: Psychological warfare is one of the earliest forms of cognitive warfare, based on the premise that perceptions and emotions are as important as physical actions in conflict. Psychological operations are used to demoralize enemy forces, influence civilians, or demoralize enemy populations. Psychological warfare can be carried out through propaganda, disinformation, rumors, and other psychological tactics. Its tactical application is the manipulation of emotions such as fear, uncertainty, and anxiety to create confusion or division within the ranks or society of the opponent. The theory emphasizes the exploitation of cognitive vulnerabilities (e.g., fear of loss, tribal instincts) to control behavior without the use of force. For example, during World War II, psychological operations were widely used by both the Axis and Allied forces to spread fear, misinformation, and demoralize enemy forces (Narula, 2004).

2- Information Warfare Theory: Information warfare deals with the control, manipulation, and distortion of information to influence cognitive processes. Information warfare is based on the assumption that information is a vital asset in modern conflicts and that whoever controls the information environment can control decision-making and behavior. This theory emphasizes attacking or defending information systems to shape the cognitive and psychological realm. Disinformation, fake news, cyberattacks on critical infrastructure, and manipulation of media narratives all play a role in modern information warfare. From a cognitive perspective, information warfare targets not only data and communication systems but also the human interpretation of that information, including the control of media and social platforms to advance particular narratives, discredit opponents, or create confusion and distrust. For example, Russia's use of disinformation and propaganda during the annexation of Crimea in 2014 is an example of information warfare. By shaping narratives through media and cyber tactics, Russia was able to influence local and international perceptions of the conflict (Bingle, 2023).

3- Cyber Psychological Warfare Theory: Cyber psychological warfare is an extension of traditional psychological warfare but conducted in cyberspace, focusing on how online information and digital tools are used to influence the thoughts, feelings, and behavior of individuals or groups. In this theory, cognitive attacks are carried out through digital platforms, often through social media, targeted disinformation, cyberbullying, or cyberterrorism. These attacks are designed to destabilize societies by spreading fake news, exacerbating divisions, or manipulating public sentiment. Social media and digital platforms serve as the battlegrounds for these operations. Cognitive manipulation is carried out by creating echo chambers, spreading disinformation, or targeting individuals with personal psychological content using data analytics and artificial intelligence. For example, Russia's alleged interference in the 2016 US presidential election is considered an example of cyber psychological warfare. Bots and trolls amplified divisive messages on social media, and misinformation campaigns were directed at specific demographic groups to manipulate voter perceptions (Crowell, 2013).

4- Behavioral Economics and Cognitive Bias Theory: This theory uses principles from behavioral economics and psychology to explain how cognitive warfare uses cognitive and heuristic biases—shortcuts in human thinking—to manipulate decision-making. Cognitive biases such as confirmation bias, availability bias, and anchoring bias make people more susceptible to misinformation and psychological manipulation. Cognitive warfare uses these natural tendencies to shape beliefs and influence actions. Arousal theory, developed by Richard Thaler and Cass Sunstein, who in their book The Savior, explain how subtle changes in the environment can affect behavior in predictable ways. In cognitive warfare, inciting populations towards desirable attitudes or behaviors (e.g., through tailored information or emotional appeals) can be very effective. For example, exploiting confirmation bias in social media algorithms that show users content that is consistent with their prior beliefs can further entrench opinions and polarize society, making them more vulnerable to cognitive manipulation (Blanco, 2017).

5- Three Wars Strategy (China): The Three Wars Strategy is a cognitive warfare framework adopted by the Chinese military that focuses on integrating psychological warfare, public opinion warfare, and legal warfare to achieve strategic objectives. Psychological warfare involves undermining the enemy's will to fight by using media and communication tools to influence perceptions. It also seeks to disrupt enemy leadership and civilian morale through psychological pressure. Public opinion warfare focuses on shaping international and domestic opinion to gain strategic advantage. Media manipulation, online influence campaigns, and narrative control play a key role in this approach. Legal warfare involves the use of international and domestic law as a tool to legitimize military

and political actions. Legal frameworks are used to control the narrative, justify operations, and exert diplomatic pressure on adversaries. For example, China's strategic use of the media to shape narratives about its actions in the South China Sea or the Belt and Road Initiative is an example of the Three Wars tactics in action. By controlling public discourse, China can sway global opinion in its favor (Mattis, 2018).

6- Narrative Warfare Theory: Narrative warfare is a theory that the control of stories—who tells them, how they are told, and how they resonate—can shape cognitive processes on a large scale. The theory assumes that humans are inherently driven by stories, and that the side that controls the dominant narrative in a conflict has a strategic advantage. Narrative warfare focuses on the framing and reshaping of events, the creation of competing narratives, and the discrediting or delegitimizing of opposing narratives. It uses storytelling to emotionally engage and persuade people, ultimately influencing their beliefs and actions. Narratives often appeal to group identity, moral values, or historical grievances, and use emotional engagement as a tool for manipulation. For example, ISIS's use of social media and digital propaganda to recruit followers through compelling narratives of resistance, martyrdom, and religious duty is an example of narrative warfare. Similarly, during the Cold War, both the United States and the Soviet Union engaged in narrative warfare to promote the superiority of their ideological systems (Aleksejeva, 2023).

7- Cognitive Load and Information Overload Theory: This theory is based on the psychological principle that humans have limited cognitive resources and can be overwhelmed by too much or contradictory information, leading to confusion, cognitive fatigue, and ultimately poor decision-making. Information overload can be used in cognitive warfare by flooding the target audience with a large volume of information, misinformation, or contradictory messages. The goal is to paralyze critical thinking, reduce trust in information sources, and lead individuals to indifference or extreme reactions. Cognitive warfare tactics in this theory include propaganda, rumors, contradictory information, or conspiracy theories, creating cognitive dissonance, and reducing individuals' ability to distinguish truth from fiction. For example, during the COVID-19 pandemic, the spread of contradictory information and conspiracy theories about the virus, vaccines, and treatments led to widespread confusion and polarization, undermining public trust in health authorities (Orru & Longo, 2019).

Research Method

This research is qualitative in terms of methodology. Given the qualitative nature of the variables under study, a descriptive-analytical method was used to conduct the research. First, by describing the research problem, we have expressed the theoretical approach and defined the research variables, and then, by referring to data collected through library resources, reputable scientific research articles, and official documents, the research data and findings have been analyzed.

Data Analysis and Research Findings

Command and Control in Warfare

Command and control is one of the most critical components of warfare, as it enables the coordination, communication, and execution of effective military operations. Command refers to the decision-making authority and process of leaders, while control includes the systems and processes that monitor, direct, and manage forces and resources during combat. The importance of command and control can be seen in several key aspects of military strategy and operations: 1- Coordination of forces in modern warfare: Modern warfare involves multiple domains—land, sea, air, cyber, and space—that require careful coordination of different branches and units. Command and control systems ensure that ground forces, air support, naval operations, and cyber warfare are coordinated to maximize effectiveness and prevent confusion or conflict between units (Black et al. 2024).

Commanders must be able to assess and respond to changing battlefield conditions in real time. Effective command and control allows for the rapid transmission of orders and information and ensures that decisions made by the leadership are immediately implemented throughout the force. 2- Efficient allocation of resources: In warfare, resources such as manpower, weapons, fuel, and supplies are limited. Command and control ensures that these resources are effectively allocated to areas where they are most needed, minimizing waste and optimizing their use. For example, ensuring that airstrikes, artillery, and infantry are used where they are most effective requires coordination through strong command and control systems. Warfare is not just about fighting, but also includes the management of logistics, transportation, and support forces. Command and control enables

commanders to monitor supply lines, move troops and equipment to where they are needed, and maintain field operations (Lucas et al. 2024). 3- Effective Communication: Command and control facilitates the flow of information between different levels of the military hierarchy, from frontline soldiers to senior leadership. Clear, accurate, and timely communication is essential to adapting to the dynamics of the battlefield and ensuring that all units understand their objectives and how they contribute to the overall strategy. Commanders must maintain situational awareness by receiving and interpreting real-time information about enemy movements, terrain, weather conditions, and friendly forces. Command and control systems help collect, analyze, and disseminate this information so that decisions are based on the most up-to-date data. 4- Control and Adaptability: Command and control systems enable adaptability in warfare. As battle conditions change—whether due to unexpected enemy movements, weather, or other factors—commanders must be able to adjust strategies and issue new orders. While central command sets the overall strategy, modern warfare often requires decentralized execution, meaning local commanders must make decisions quickly. Command and control ensures that they have the authority and information necessary to act while still adhering to the larger strategic plan (Military Protocol, 2024).

5-Integration and convergence of actions: Command and control ensures that all military efforts are aligned with overall strategic objectives. Without a coherent command and control structure, units or branches may pursue conflicting goals, leading to inefficiency or even failure. Large-scale operations require the synchronization of multiple units, often spread over large areas. Command and control helps synchronize these actions so that operations are carried out in a coordinated manner and achieve the greatest possible impact. For example, an amphibious assault may require coordination of naval, air, and land forces, which is only possible through an effective command and control framework (apps, 2021).

6-Discipline and control over forces: Command and control allows for the monitoring and enforcement of discipline within the military ranks. Orders must be consistently followed, and leaders must have the means to ensure that all units adhere to rules of engagement, operating procedures, and strategic objectives. In the heat of battle, the risk of chaos and confusion is high. Without effective control, units may become disorganized, misinterpret orders, or act independently of the larger strategy, leading to failure. Command and control systems prevent such breakdowns by ensuring continuous control over forces (U.S. Marine Corps, 2018).

7-Use of modern systems: Modern military operations increasingly rely on advanced technologies such as drones, satellites, and cyber capabilities. Command and control systems integrate these technologies, allowing commanders to monitor the battlefield, conduct precision strikes, and defend against cyber threats. The integration of artificial intelligence and data analytics into command and control systems is also becoming more common, enabling faster decision-making and better resource management. As warfare becomes digital, cyber operations play a critical role in offensive and defensive strategies. A robust command and control framework ensures that military systems are protected from cyber attacks and that cyber operations are synchronized with physical operations (Totalmilitaryinsight, 2024).

8-Moral and psychological impacts: Commanders play a critical role in maintaining morale among troops. Effective communication, clear leadership, and coordinated actions help soldiers feel confident about their mission and their chances of success. Good command and control helps prevent confusion and uncertainty, which can lead to demoralization. Command and control also helps with psychological operations by controlling the narrative and ensuring that information is communicated in ways that affect both friendly and adversary forces. Leaders can use command and control to project power, spread disinformation, or demoralize an enemy with strategic communications (Zucker and RowelL, 2021).

9-The link between military and political strategy: Command and control serves as a bridge between political goals and military action. Command and control ensures that military operations are aligned with a nation's broader political and diplomatic goals, enabling leaders to tailor strategies to achieve not only battlefield victories but also long-term political success. In conflicts, especially those involving nuclear or other strategic weapons, command and control systems are critical to ensuring that decisions around escalation are deliberate and controlled. Effective command and control helps prevent accidental or unauthorized escalation and maintains strategic stability (Vego, 2024).

10-Countering Asymmetric Threats: In modern conflicts, many adversaries are non-state actors who use guerrilla tactics, terrorism, or cyberattacks. Command and control systems enable military forces to manage these

asymmetric threats by coordinating intelligence, counterterrorism, and cyberdefense efforts. In asymmetric warfare, where traditional military power may not be effective, command and control systems help manage intelligence, civil-military relations, and local security forces to counter insurgencies. These operations require a high level of coordination between military, intelligence, and civilian entities. The importance of command and control in warfare cannot be overstated as it is the backbone of military operations that enables coordination, communication, and execution of complex strategies. By providing a structured system for leadership to exercise authority, communicate decisions, allocate resources, and adapt to changing circumstances, command and control ensures that military forces can operate coherently and efficiently, maximizing their chances of success in conflict. In modern warfare, where the speed and complexity of operations continue to increase, command and control remains a critical element of military power and strategic effectiveness (Dodcio, 2020).

The EU Approach to Command and Control of War

The EU's approach to command and control of military operations reflects its unique nature as a political and economic union of independent states. Unlike traditional nation-states with a unified military command structure, the EU's defence and security framework operates through a consensus-based system, where member states voluntarily share forces and resources. This approach is formalised in the EU's Common Security and Defence Policy. The EU's command and control of military operations is characterised by a cooperative, decentralised and multilateral structure, with an emphasis on political control, multinational coordination and interoperability (Bond & Scazzieri, 2022).

1- The Common Security and Defence Policy is the EU's main mechanism for managing defence and security activities, including military missions and operations, providing the organisational and operational framework for how the EU coordinates command and control in military conflicts. Military operations under the Common Security and Defence Policy are subject to strong political control by EU member states. The EU Political and Security Committee, composed of representatives of the Member States, plays a key role in providing political guidance and control throughout the operational cycle. Member States decide on a case-by-case basis to contribute forces or resources to EU Common Security and Defence Policy operations. This means that the EU's military command and control depends largely on the collective political will of its members rather than on a single, permanent military structure (Bergmann & Müller, 2021).

2- The EU Military Staff and Command Structures The EU Military Staff is the main military planning and operations body in the EU, playing a key role in coordinating command and control for EU operations. The EU Military Planning and Conduct Capability was established to strengthen the EU's ability to plan and conduct military operations. It acts as the operational headquarters for EU missions and ensures command and control for non-executive operations such as training missions. However, for larger military operations, the EU Military Planning and Conduct Capability is coordinated with national headquarters provided by the Member States. Operational Headquarters In CSDP missions, actual command and control is usually delegated to an operational headquarters, which can be a national or multinational headquarters. For example, a member state may offer its military headquarters to serve as the operational headquarters for a specific mission (Palm & Crum, 2019).

3- The EU Military Committee is the highest military body in the EU Common Security and Defence Policy structure, composed of the heads of defence of the EU member states. It provides military advice and guidance for EU military operations. The EU Military Committee advises the EU Political and Security Committee and monitors the implementation of military decisions taken by the Council of the EU. It also ensures that the planning and execution of military operations are aligned with the EU's strategic objectives (Barigazzi, 2024).

4- Multinational forces: A key feature of the EU approach to command and control is the use of multinational forces, which emphasises interoperability between the diverse military forces of the member states. The concept of the EU Battlegroup, developed in the early 2000s, is a prime example of multinational cooperation under the EU command structure. These battlegroups are rapid reaction military units, each led by a framework country and involving contributions from several member states. They were previously designed for deployment in specific crisis scenarios, but were never used, largely due to the political challenges surrounding their activation. Given that EU member states use different military systems, languages, and doctrines, the EU places significant emphasis on interoperability and ensuring that forces can work together under a unified command structure. Command and

control systems are designed to allow multinational forces to seamlessly communicate and coordinate actions on the battlefield (Palm & Crum, 2019).

5- Coordination with NATO: Given that many EU member states are also NATO members, there is close coordination between EU command and control structures and the NATO framework. This coordination helps to avoid duplication and ensures that EU and NATO operations are complementary rather than competitive. The Berlin Plus Agreement allows the EU to access NATO planning capabilities and assets for military operations where NATO is not involved. It provides a framework for EU and NATO cooperation in command and control and ensures that EU-led operations can benefit from NATO's extensive command and control infrastructure. While NATO remains the primary military alliance for European security, the EU has developed its own command and control capabilities for missions falling under the EU's Common Security and Defence Policy, in particular those related to crisis management, peacekeeping, and humanitarian missions (Clingendael Report October, 2021).

6. Civil-Military Coordination

A defining feature of the EU approach to command and control is its emphasis on the integration of civilian and military capabilities, known as the comprehensive approach. The EU conducts military and civilian missions, often simultaneously, which requires strong coordination between the two domains. Many operations under the EU's Common Security and Defence Policy include civilian components, such as police training, rule of law initiatives and institution-building. These missions are often conducted in parallel with military operations and require effective command and control structures that can integrate civilian and military efforts. The EU emphasizes civil-military coordination at all levels of command. The EU's Crisis Management and Planning Directorate plays a key role in ensuring that civilian and military operations are planned and implemented in a complementary manner (Palm & Crum, 2019).

7. Crisis Response Operations

The EU's command and control approach is designed to respond to crises, both inside and outside Europe. While the EU does not have a standing army, it can mobilize member states' forces to carry out peacekeeping, stability and crisis management missions. Regional focus: Many EU operations focus on crisis areas in Africa, the Balkans and the Middle East. The EU's military operations in Mali and Somalia and Bosnia and Herzegovina (Operation Althea) are examples of how the EU can command and control international crises (Bergmann & Müller, 2021).

In recent years, the EU has sought to increase its ability to conduct military operations independently of NATO, a concept known as strategic autonomy. The Permanent Structured Cooperation initiative, launched in 2017, is part of this effort, which aims to deepen defense cooperation and improve the EU's collective capabilities, including command and control. The EU's approach to command and control in war is not without its challenges, however, largely due to the political and structural complexities of coordinating military action across 27 independent states. One of the main limitations of the EU's command and control structure is the need for political consensus. Any major military operation requires unanimous agreement among EU member states, which can delay decision-making and deployment. Unlike a traditional military force under a single command, EU military operations are often a combination of contributions from different member states, which can lead to challenges in terms of coordination, logistics, and command authority, especially in complex or high-risk operations. The EU's approach to command and control in war reflects its unique structure as a supranational organization of sovereign states. The EU operates through a decentralized and multilateral command and control framework, focusing on political control, multinational coordination, and military-military integration. While the EU approach has limitations, particularly related to political consensus and the lack of a standing army, it enables the Union to respond to crises, manage peacekeeping missions, and enhance European security in cooperation with NATO and other international partners. The EU's efforts towards strategic autonomy and deep defense cooperation suggest that its command and control capabilities will continue to evolve in the years to come (Juncos & Blockmans, 2018).

Command and Control Approaches to Cognitive Warfare

Different countries adopt different approaches to command and control of cognitive warfare, based on geopolitical objectives, political systems, and military doctrines. Countries such as the United States, Russia, and China have developed comprehensive strategies that integrate cognitive warfare into broader defense frameworks, while countries such as France, the United Kingdom, and the Zionist regime use cognitive techniques as part of

asymmetric, cyber, or infiltration operations. As cognitive warfare becomes increasingly important, command and control structures will continue to evolve, incorporating advanced technologies and information systems to shape the cognitive domain of future conflicts (Niven, 2021). Here is an overview of how different countries approach command and control of cognitive warfare:

1-United States: The United States has been a leader in developing strategies to address cognitive warfare, particularly within the broader military doctrine of information operations and psychological operations. The United States considers cognitive warfare to be part of its multi-domain operations that seek to integrate military efforts across land, sea, air, cyber, and cognitive domains. The United States Department of Defense considers cognitive warfare to be part of its overall strategy to achieve superiority in all domains. United States Cyber Command and other military branches, such as the Army and Air Force, have integrated cognitive operations into their strategic frameworks. Cognitive warfare is seen as a means of shaping adversary perceptions, influencing decision-making, and neutralizing threats before they escalate into kinetic conflict. Cognitive warfare command and control is distributed across multiple organizations and branches, including the Joint Intelligence Operations Center and the United States Cyber Command, but as cognitive intelligence is also deeply intertwined with the Central Intelligence Agency (CIA) and the State Department, it can be said that warfare intersects with intelligence and diplomacy. The United States is increasingly using artificial intelligence and big data to enhance its cognitive warfare capabilities. The Department of Defense is investing in data analytics, social media monitoring, and psychological profiling to influence hostile populations and counter disinformation (Hall, 2023).

2-Russia: Russia is a major proponent of cognitive warfare, often referred to as information warfare or hybrid warfare. The Russian military and intelligence services use cognitive warfare as a key tool to undermine adversaries without direct military confrontation. The command and control of cognitive warfare in Russia is tightly controlled by its Military Intelligence Agency, the military's Foreign Intelligence Service, and the Federal Security Service. These agencies are responsible for conducting disinformation campaigns, psychological operations, and political intervention in foreign countries. The Kremlin exercises close control over these operations to ensure alignment with Russia's geopolitical goals.

Russia's cognitive warfare strategies are heavily focused on disinformation and narrative manipulation, which includes the use of state-controlled media outlets (such as Russia Today and Sputnik), social media campaigns, and trolls to spread misleading or false information, particularly in Western democracies. Russian military thinkers, most notably General Valery Gerasimov, have advocated cognitive warfare as part of Russia's broader strategy of nonlinear warfare or hybrid warfare. This approach seeks to blur the lines between war and peace, using intelligence and psychological operations to destabilize adversaries without overt conflict (Splidsboel Hansen, 2021).

3-China: China views cognitive warfare as part of its three-war strategy – public opinion warfare, psychological warfare, and legal warfare. The goal of winning without war is to use cognitive techniques to shape perceptions at home and abroad, influence international law, and undermine the resolve of adversaries. Cognitive warfare operations in China are centrally controlled by the Chinese Communist Party through the Propaganda Department, the Strategic Support Force of the People's Liberation Army, and the United Front Work Department. These organizations are responsible for information control, public opinion management, and psychological warfare (Hung & Hung, 2022).

One of China's main goals is to control the narrative about China domestically and internationally, which includes efforts to influence global media, diplomacy, and online discourse to ensure that China's rise is perceived positively and criticism is minimized. The use of social media platforms and state-sponsored cyber campaigns to shape global opinion has become central to China's strategy. China's approach to cognitive warfare extends to psychological operations aimed at demoralizing potential adversaries, as well as legal warfare that seeks to manipulate international legal frameworks to serve China's interests. Cognitive warfare is also embedded in China's Belt and Road Initiative, where information penetration is part of the expansion of soft power.

4-UK: The UK has incorporated cognitive warfare as part of its broader defense and security strategy, recognizing it as a fundamental aspect of information superiority. Cognitive warfare is closely linked to the UK's cyber defense and counter-disinformation strategies. The UK's Fusion Doctrine, introduced in the 2018 National Security Capability Review, integrates cognitive warfare with cyber defence, intelligence and military operations. The

doctrine emphasises whole-of-government coordination and ensures that all tools of governance – diplomatic, economic, military and intelligence – are deployed in cognitive warfare. Agencies such as MI5 (domestic intelligence) and the Government Communications Headquarters, which manages signals intelligence and cyber operations, are key players in cognitive warfare. These agencies use cognitive techniques to disrupt terrorist recruitment, counter extremist ideologies and defend against hostile information campaigns. The UK has prioritised countering Russian disinformation and Chinese infiltration operations. The Rapid Response Unit (part of the Cabinet Office) monitors and counters disinformation in real time, while 77 Brigade, a British Army unit, focuses on psychological operations and shaping public narratives (Reding & Wells, 2022).

5-France: France has embraced cognitive warfare in its broader concept of cyber defense and infiltration operations, which are increasingly integrated into its military doctrine. In its approach to cognitive warfare, France emphasizes strategic independence and maintains independent capabilities to influence the information space. The French military considers cognitive warfare essential to maintaining freedom of action in both national defense and NATO operations. The French Military Intelligence Directorate and Cyber Command are responsible for conducting infiltration operations. France focuses on protecting national narratives, combating extremist propaganda, and participating in counter-extremism efforts. The country prioritizes narrative control in its cognitive warfare strategy, particularly in regions such as Africa, where it has long-standing geopolitical interests. The French military uses infiltration operations to protect its interests in the Sahel, where cognitive warfare is used to counter Islamist insurgencies (they claim) and to reduce the influence of Russia and China (Claverie & Du Cluzel, 2022).

6- Israel: Israel views cognitive warfare as a fundamental component of its asymmetric warfare strategy. In confronting the resistance front forces, namely Hamas and Hezbollah, the Israeli regime uses cognitive operations to disrupt their decision-making, undermine their morale, and influence international perceptions of them. The Israeli regime's cognitive warfare efforts are largely led by military intelligence, particularly Unit 8200, which is responsible for cyber and intelligence operations. The regime integrates cognitive warfare into broader intelligence operations and uses targeted messaging and psychological operations to undermine the enemy's resolve and control the narrative. The Israeli regime places great emphasis on perception management to ensure that its actions are seen as justified and legitimate on the global stage, which includes efforts to shape media coverage of conflicts, counter hostile narratives, and influence international public opinion (Mackiewicz, 2019).

The EU Approach

The EU's approach to command and control of cognitive warfare is still evolving, reflecting the wider complexities of its defence and security structures. Cognitive warfare is considered part of the EU's broader efforts in information security, hybrid threats and strategic communications, but unlike some countries, it does not have a fully focused or military-focused doctrine in this area. Instead, the EU addresses cognitive warfare through coordinated civilian, military and diplomatic efforts, often in cooperation with NATO and nation-states. This includes countering disinformation, protecting democratic processes, and ensuring resilience against hybrid and information warfare. The main components of the EU's approach to cognitive warfare are:

1-Hybrid threats and information warfare: The EU sees cognitive warfare as part of a broader category of hybrid threats – a combination of conventional and unconventional means to undermine societies that include disinformation, cyberattacks and psychological manipulation, often seen in the context of threats from state and non-state actors such as Russia or terrorist groups. The European Centre of Excellence for Countering Hybrid Threats, based in Helsinki, Finland, plays a key role in addressing cognitive warfare by analysing hybrid warfare tactics and developing strategies to counter them. The centre works with the EU and NATO to provide member states with information and training to counter cognitive threats, including disinformation campaigns and psychological operations. The EU established a hybrid office, the Hybrid Fusion Office, within the European External Action Service to improve the analysis and understanding of hybrid threats, including cognitive warfare. The office monitors and responds to disinformation and attempts to manipulate public opinion across the EU (Glasser et al. 2023).

2-Disinformation and strategic communications: The EU is strongly focused on countering disinformation campaigns aimed at undermining public trust in institutions, democracy and political systems. The EU has prioritized this aspect of cognitive warfare in recent years due to the increased activity of foreign actors,

particularly Russia, in influencing elections and spreading false narratives. STRATCOM Task Force East is one of the leading bodies addressing cognitive warfare, particularly Russian disinformation in Eastern Europe. It was established in 2015 to monitor and counter disinformation campaigns by foreign actors targeting the EU and its member states. The task force focuses on providing accurate information, developing counter-narratives, and raising awareness of cognitive threats. The EU Campaign and Disinformation The EU Initiative Against Disinformation, part of STRATCOM Task Force East, focuses on exposing and refuting disinformation to EU citizens. By monitoring media and social networks, it helps to increase the EU's resilience against cognitive warfare by ensuring citizens have access to verified information (Casero-Ripollés et al. 2023).

3- Cybersecurity and Cognitive Resilience: While the EU approach to cognitive warfare focuses on information and narrative control, it is also closely linked to cybersecurity and the protection of critical infrastructure. Cognitive warfare tactics often include cyber elements such as hacking, data manipulation, and the use of social media platforms to spread disinformation. In 2020, the European Union updated its cybersecurity strategy to counter hybrid and cognitive threats. The strategy emphasizes strengthening the cyber resilience of member states and ensuring that civilian and military infrastructure is protected against information manipulation and disinformation campaigns. The EU also operates cyber rapid response teams designed to help member states counter cybersecurity threats and cognitive warfare. These teams can be deployed to respond to hybrid and cognitive attacks, such as those involving disinformation and manipulation of online content (Giannopoulos et al. 2020).

4-Democratic resilience and electoral security: Another key area where the EU addresses cognitive warfare is ensuring electoral security and protecting democratic processes from external interference. Foreign actors, notably Russia, have been accused of attempting to influence elections and referendums in EU countries through disinformation and psychological manipulation, leading to coordinated efforts to protect elections from cognitive attacks (European Parliament, 2023).

5-The European Democracy Action Plan, launched in 2020, is the EU's response to growing concerns about cognitive warfare tactics that undermine democratic institutions. It focuses on countering disinformation, protecting electoral integrity, and promoting media literacy, including measures to increase transparency in political advertising and strengthen cooperation between member states in responding to cognitive warfare (Calabrese et al. 2023).

6-Cooperation with social media platforms: The EU works closely with major social media platforms such as Facebook, Twitter and Google to counter cognitive threats. These platforms are seen as central battlegrounds for cognitive warfare, as they are often used to spread disinformation and manipulate public opinion. The Code of Conduct on Disinformation, introduced in 2018, aims to hold these platforms accountable for monitoring and removing harmful content, especially during sensitive periods such as elections (Goujard, 2023). 6. Multinational cooperation: The EU's approach to cognitive warfare is strongly based on multilateralism and international cooperation. It works with NATO, the United Nations and individual member states to address the global nature of cognitive threats. Given that many EU members are also members of NATO, there is a close relationship between the two organizations in addressing cognitive and hybrid warfare. NATO's strategic communications, cyber defense, and resilience initiatives often align with EU efforts to counter cognitive threats. The European Defense Fund supports innovation in military technology, including cognitive warfare tools, which include the development of AI-based intelligence analytics, tools to detect disinformation, and increased resilience of communications infrastructure (Miller, 2023).

7-Military and intelligence integration: Although the EU's approach to cognitive warfare is largely civilian, it has made efforts to integrate military capabilities into its strategy where necessary. Cognitive warfare overlaps with military operations, particularly in psychological operations and information warfare in conflict zones. EU member states are developing joint military capabilities in the form of Permanent Structured Cooperation, including those addressing cognitive and hybrid threats. Permanent Structured Cooperation projects related to cyber defense and information sharing enhance the EU's ability to counter cognitive warfare by improving coordination between military and intelligence services across Europe. The EU Intelligence and Situation Centre plays a key role in monitoring cognitive warfare threats by collecting and analysing information on combined operations, including disinformation and psychological operations campaigns targeting EU Member States. It

provides strategic intelligence and supports EU decision-making in the face of cognitive warfare threats (Reding & Wells, 2022).

8-Focus on media literacy and public awareness: One of the EU's long-term active strategies in countering cognitive warfare is media literacy and public awareness campaigns. The aim is to ensure that citizens can recognise and resist disinformation, fake news and manipulation. The EU supports various media literacy initiatives to teach citizens how to critically assess information. These initiatives are particularly aimed at vulnerable populations, such as young people and the elderly, who are often the main targets of disinformation campaigns. The EU Digital Services Act, adopted in 2022, is an ambitious law that aims to regulate online platforms and ensure that they are held accountable for the dissemination of illegal content, including disinformation. By requiring platforms to increase transparency about how they moderate content and use algorithms, the EU seeks to minimize the effects of cognitive warfare tactics that exploit social media networks (Pamment, 2020).

Conclusions

The EU's approach to command and control of cognitive warfare is based on multinational cooperation, information security and building focused resilience. While the EU lacks a unified military command structure for cognitive warfare, it uses its civilian institutions, cyber defence mechanisms and strategic communication capabilities to protect its member states against the growing threats of disinformation, hybrid attacks and psychological manipulation. The emphasis on democratic resilience, public awareness and international cooperation underlines the EU's recognition of cognitive warfare as a key challenge in modern security policy. The EU recognises cognitive warfare as part of a broader range of hybrid threats that include disinformation, cyber attacks and political subversion. The EU Hybrid Threat Strategy and the EU Action Plan on Disinformation provide frameworks for understanding and countering cognitive manipulation. These strategies highlight the importance of securing the information space, strengthening resilience and building public trust through transparent and credible communications. Resilience against cognitive warfare involves increasing the public's ability to identify, understand and respond to disinformation and psychological influences. The EU emphasises digital sovereignty and protects its citizens from external malign influence by promoting European control over key digital infrastructure, technologies and platforms. Cognitive warfare for the EU overlaps with cybersecurity. As a result, the EU Cybersecurity Strategy identifies threats to digital infrastructure and information systems that can be exploited in cognitive operations. The EU Cybersecurity Agency plays a role in developing policies and practices to protect against cyber cognitive threats. The EU works closely with NATO in addressing cognitive warfare as part of hybrid warfare. NATO's Cognitive Warfare Initiative and its focus on strategic communications, information warfare and psychological operations complement the EU's efforts. The EU also supports member states in developing national capabilities to counter cognitive threats through training, information sharing and better methods and practices. Another key element of the Union's fight against cognitive warfare is improving media literacy among EU citizens. For example, the EU's Digital Education Action Plan and the Media Literacy for All Programme aim to equip individuals with the skills needed to critically assess the information they consume, making it more difficult for adversaries to manipulate or control public opinion. The EU's approach to cognitive warfare is also based on its commitment to democratic principles, human rights and the rule of law, and therefore command and control strategies must balance the need for security with the protection of fundamental freedoms such as freedom of expression and privacy. The EU's General Data Protection Regulation is an example of the EU's efforts to protect citizens' data from misuse in psychological or cognitive operations. Given that the EU sees cognitive warfare increasingly using artificial intelligence and machine learning, the EU's Artificial Intelligence Strategy includes provisions to address the ethical use of artificial intelligence, in particular in defence and security, and to counter the potential misuse of artificial intelligence in cognitive manipulation.

Based on the results of this study, it is suggested that the following issues be placed on the agenda of academic and executive institutions;

- Paying serious attention to emerging technologies such as artificial intelligence and its potential for use in cognitive warfare, as well as command and control of this war

- Addressing media and media literacy issues from a geopolitical perspective, and not just technical and skill-based issues of media and information literacy

- Launching digital mobilization to involve people and citizens in confronting cognitive warfare

- Planning and managing election security and protecting democratic processes from foreign cognitive interference

- Cooperating with social media platforms to counter disinformation, including fake news and political propaganda

- Paying attention to multilateralism and international cooperation for cognitive warfare management

-Teaching the correct concept of cognitive warfare, taking into account the overlap of cognitive warfare with military operations, especially in psychological operations and information warfare in conflict zones

References

[1] Apps, (2021). Defense Primer: What Is Command and Control?, https://apps.dtic.mil/sti/pdfs/AD1132997.pdf#:~:text=The%20Department%20of%20Defense%20%28DOD%29%20defines%20command%20and,level%2C%20C2%20represents%20how%20DOD%20makes%20operational%20decisions.

[2] Barigazzi, J. (2024). Neutral-country general to head EU's top military body, https://www.politico.eu/article/neutral-country-general-sean-clancy-head-eu-top-military-body-european-union-military-committee/

[3] Bergmann, J., & Müller, P. (2021). Failing forward in the EU's common security and defense policy: the integration of EU crisis management. Journal of European Public Policy, 28(10), 1669–1687. https://doi.org/10.1080/13501763.2021.1954064

[4] Bergmann, J., & Müller, P. (2021). Failing forward in the EU's common security and defense policy: the integration of EU crisis management. Journal of European Public Policy, 28(10), 1669–1687. https://doi.org/10.1080/13501763.2021.1954064

[5] Bingle, Morgan(2023). What is Information Warfare?, https://jsis.washington.edu/news/what-is-information-warfare/

[6] Black, J., Lucas, R. Kennedy, J. Hughes, M. and Fine, H..(2024) Command and Control in the Future: Concept Paper 1: Grappling with Complexity, RAND Corporation, RR-A2476-1, 2024. As of October 11, 2024: https://www.rand.org/pubs/research_reports/RRA2476-1.html

[7] Blanco, F. (2017). Cognitive Bias. 10.1007/978-3-319-47829-6_1244-1.

[8] Bond, I. & Scazzieri, L.(2022). The EU, NATO and European security in a time of war, https://www.cer.eu/publications/archive/policy-brief/2022/eu-nato-and-european-security-time-war

[9] Buvarp, P.M.H.(2023). Mitigating and Responding to Cognitive Warfare, Technical Evaluation Report (TER) HFM-361,Research Symposium (RSY)

[10] Calabrese, S., Smith, L., Antoniou, E., Johnson, C., (2023). Reviewing progress on the European Democracy Action Plan, https://capacity4dev.europa.eu/library/reviewing-progress-european-democracy-action-plan_en#:~:text=On%203%20December%202020%20the%20European%20Commission%20published,fair%20elections%3B%20strengthening%20media%20freedom%3B%20and%20countering%20disinformation

[11] Casero-Ripollés, A., Tuñón, J. & Bouza-García, L.)2023(. The European approach to online disinformation: geopolitical and regulatory dissonance. Humanit Soc Sci Commun 10, 657 (2023). https://doi.org/10.1057/s41599-023-02179-8

[12] Claverie, B. & Du Cluzel, F.(2022).Cognitive Warfare: The Advent of the Concept of "Cognitics" in the Field of Warfare. Bernard Claverie; Baptiste Prébot; Norbou Buchler; François du Cluzel. Cognitive Warfare: The Future of Cognitive Dominance, NATO Collaboration Support Office, pp.2, 1-7, 2022, 978-92-837-2392-9. ffhal-03635889f

[13] Clingendael Report October, (2021). EU-NATO cooperation: what has been achieved so far?, https://www.clingendael.org/pub/2021/countering-hybrid-threats/3-eu-nato-cooperation-what-has-been-achieved-so-far/

[14] Crowell, R. M.(2017). Some Principles of Cyber Warfare Using Corbett to Understand War in the Early Twenty–First Century, The Corbett Centre for Maritime Policy Studies, Corbett Paper, No 19

[15] dodcio, (2020). Command, control, and communications (C3) systems, https://dodcio.defense.gov/Portals/0/Documents/DoD-C3-Strategy.pdf

[16] Editorial Team.(2024). The Impact of Propaganda in World War I: A Historical Analysis, https://totalmilitaryinsight.com/propaganda-in-world-war-i/#
[17] Engerman, D. (2010). Ideology and the origins of the Cold War, 1917–1962. In M. P. Leffler & O. A. Westad (Eds.), The Cambridge History of the Cold War (pp. 20–43). chapter, Cambridge: Cambridge University Press.
[18] Europa, (2024). Cognitive warfare in the new international competition: an emerging challenge for the EU PILOT Course: https://esdc.europa.eu/2024/05/28/cognitive-warfare-in-the-new-international-competition-an-emerging-challenge-for-the-eu-pilot-course/
[19] European Parliament, (2023), REPORT on foreign interference in all democratic processes in the European Union, including disinformation, https://www.europarl.europa.eu/doceo/document/A-9-2023-0187_EN.html
[20] Fabio & Rhode, Steffen & Daseking, Monika. (2023). A Systematic Review Of Cognitive And Psychological Warfare. 10.5281/zenodo.10205600.
[21] Giannopoulos, G., Smith, H.(2020), Theocharidou, M., The Landscape of Hybrid Threats: A conceptual model, European Commission, Ispra, 2020, PUBSY No. 123305
[22] Glasser, G. & Rickli, J.-M. & Mantellassi, F. (2023). Peace of Mind: Cognitive Warfare and the Governance of 21st Century Subversion. https://www.researchgate.net/publication/373389102_Peace_of_Mind_Cognitive_Warfare_and_the_Governance_of_21st_Century_Subversion
[23] Goujard, C.(2023). Facebook, Twitter to face new EU content rules by August 25, https://www.politico.eu/article/facebook-twitter-to-face-new-eu-content-rules-by-august-25/
[24] Hall, Daniel S. (2023). America Must Engage in the Fight for Strategic Cognitive Terrain, https://ndupress.ndu.edu/Media/News/News-Article-View/Article/3264639/america-must-engage-in-the-fight-for-strategic-cognitive-terrain/
[25] Hung, T.-C., Hung, T.-W. (2022). How China's Cognitive Warfare Works: A Frontline Perspective of Taiwan's Anti-Disinformation Wars, Journal of Global Security Studies, Volume 7, Issue 4, December 2022, ogac016, https://doi.org/10.1093/jogss/ogac016
[26] Jones, A. (2011). Psychological Observations of Napoleon Bonaparte, https://www.historicmysteries.com/history/napoleon-bonaparte/1404/
[27] Juncos, A. E., & Blockmans, S. (2018). The EU's role in conflict prevention and peacebuilding: four key challenges. Global Affairs, 4(2–3), 131–140. https://doi.org/10.1080/23340460.2018.1502619
[28] Mackiewicz, D. (2019). Cognitive Warfare, Conference: INSS-Summer Institute 2018At: Tel Aviv, Israel
[29] Mattis, P.(2018). China's 'Three Warfares' in Perspective, https://warontherocks.com/2018/01/chinas-three-warfares-perspective/
[30] Military Protocol, (2024). Understanding the Chain of Command Structure in Military Operations, https://totalmilitaryinsight.com/chain-of-command-structure/
[31] Miller, S. (2023). Cognitive warfare: an ethical analysis. Ethics Inf Technol 25, 46. https://doi.org/10.1007/s10676-023-09717-7
[32] Miller, S..(2023). Cognitive warfare: an ethical analysis. Ethics Inf Technol 25, 46. https://doi.org/10.1007/s10676-023-09717-7
[33] Mottaghi Dastenaei, Afshin, Karami, Ali (2024), The Depth of Digital Geopolitics (Volume One), Tehran: Kharazmi University Press.
[34] Narula, S. (2004). Psychological operations (PSYOPs): A conceptual overview. Strategic Analysis, 28(1), 177–192. https://doi.org/10.1080/09700160408450124
[35] Niven, G.(2021). The Anatomy of Command and Control:a Generic Functional Model, https://assets.publishing.service.gov.uk/media/65e84b114e2a8a00115c37a2/Anatomy_of_Command_and_Control_GOV.pdf
[36] Orru, G. & Longo L. (2019). "The Evolution of Cognitive Load Theory and the Measurement of Its Intrinsic, Extraneous and Germane Loads: A Review". Human Mental Workload: Models and Applications. Communications in Computer and Information Science. Vol. 1012. pp. 23–48. doi:10.1007/978-3-030-14273-5_3. ISBN 978-3-030-14272-8. S2CID 86587936. {{cite book}}: |journal= ignored (help)
[37] Palm, T., & Crum, B. (2019). Military operations and the EU's identity as an international security actor. European Security, 28(4), 513–534. https://doi.org/10.1080/09662839.2019.1667769

[38] Palm, T., & Crum, B. (2019). Military operations and the EU's identity as an international security actor. *European Security*, *28*(4), 513–534. https://doi.org/10.1080/09662839.2019.1667769

[39] Palm, T., & Crum, B. (2019). Military operations and the EU's identity as an international security actor. European Security, 28(4), 513–534. https://doi.org/10.1080/09662839.2019.1667769

[40] Pamment, J.(2020).The EU's Role in Fighting Disinformation: Taking Back the Initiative, https://carnegieendowment.org/research/2020/07/the-eus-role-in-fighting-disinformation-taking-back-the-initiative?lang=en

[41] Reding, D.F., Wells, B. (2022). Cognitive Warfare: NATO, COVID-19 and the Impact of Emerging and Disruptive Technologies. In: Gill, R., Goolsby, R. (eds) COVID-19 Disinformation: A Multi-National, Whole of Society Perspective. Advanced Sciences and Technologies for Security Applications. Springer, Cham. https://doi.org/10.1007/978-3-030-94825-2_2

[42] Reding, D.F., Wells, B. (2022). Cognitive Warfare: NATO, COVID-19 and the Impact of Emerging and Disruptive Technologies. In: Gill, R., Goolsby, R. (eds) COVID-19 Disinformation: A Multi-National, Whole of Society Perspective. Advanced Sciences and Technologies for Security Applications. Springer, Cham. https://doi.org/10.1007/978-3-030-94825-2_2

[43] Splidsboel Hansen, F. (2021). When Russia Wages War in the Cognitive Domain. The Journal of Slavic Military Studies, 34(2), 181–201. https://doi.org/10.1080/13518046.2021.1990562

[44] totalmilitaryinsight, (2024). Harnessing Drone Technology in Combat: A New Era of Warfare, https://totalmilitaryinsight.com/drone-technology-in-combat/

[45] U.S. Marine Corps, (2018). Command and Control, DEPARTMENT OF THE NAVY Headquarters United States Marine Corps Washington, D.C. 20350-3000

[46] van der Klaauw, C. (2023), cognitive warfare, https://www.jwc.nato.int/application/files/7216/9804/8564/CognitiveWarfare.pdf

[47] Vego, M.(2024). Converting a Political- to a Military-Strategic Objective, https://ndupress.ndu.edu/Media/News/News-Article-View/Article/3680005/converting-a-political-to-a-military-strategic-objective/

[48] Zucker, R. and Rowell, D.(2021). Decision making and problem solving, 6 Strategies for Leading Through Uncertainty, https://hbr.org/2021/04/6-strategies-for-leading-through-uncertainty