Policy Brief No150924

HYBRID AND COGNITIVE WARFARE:

GLOBAL SECURITY CHALLENGES

Wissal Rida

September 2024

Policy Brief No150924

HYBRID AND COGNITIVE WARFARE: GLOBAL SECURITY CHALLENGES

Wissal Rida
Wissalr@youthpolicycenter.org

September 2024

ABSTRACT

In the intricate and constantly evolving landscape of contemporary conflicts, nations across the globe find themselves standing at a crucial juncture, positioned within a complex and multifaceted battleground. This arena is no longer defined by traditional weaponry but rather by the nuanced and potent tools of cognitive and hybrid warfare. In this theater, the influence of ideas and information often eclipses the purely military aspect from a strategic standpoint. History attests to the fact that a conflict can be won on the battlefield yet lost on the front of public opinion. Here, the tools of disinformation, cyberattacks, and psychological manipulation wield a substantial influence. Many nations, like those discussed in this paper, confront these formidable adversaries. Within this context, we embark on an academic exploration of the profound challenges and research-based recommendations pertaining to cognitive and hybrid warfare in this unfamiliar domain.

Keywords: Cognitive Warfare, Hybrid Warfare, Disinformation…

INTRODUCTION

In today's increasingly interconnected world, traditional concepts of warfare have significantly evolved. The conventional battlefields of the past, with clear-cut frontlines and uniformed combatants, have given way to a new era where adversaries operate in the shadows, yet equally potent weapons: *hybrid and cognitive warfare.*

Hybrid warfare is a multifaceted strategy that merges conventional and unconventional warfare. It combines traditional military tactics with cyberattacks, disinformation campaigns, and proxy forces. This versatile approach challenges the foundations of national security by making it difficult to identify the instigators or blurring battle lines. On the other hand, cognitive warfare focuses on the manipulation of perception. It targets public opinion by disseminating disinformation, influencing beliefs, and creating societal divisions.

The consequences of these tactics are not confined by borders. They have profound global significance. Hybrid and cognitive warfare surpass the confines of individual nations, affecting countries worldwide and complicating the dynamics of international relations. These strategies undermine trust, national sovereignty, and democratic processes, fundamentally altering the nature of modern conflicts.

Within this ever evolving and intricate global security landscape, it becomes imperative to develop a thorough understanding of the complexities of hybrid and cognitive warfare. This policy brief is designed to provide an in-depth analysis of these emerging threats, and their impact on international security. It also offers practical recommendations to navigate the intricate domain of hybrid and cognitive warfare. To achieve this, we will explore the facets of these challenges, drawing insights from real-world examples and examining the varied international responses. This brief seeks to equip policymakers with insights to navigate these threats and protect global security in an increasingly complex and uncertain era.

RESEARCH OVERVIEW

Hybrid and cognitive warfare have become central to modern global security. These forms of warfare are dynamic and multifaceted. The term "hybrid warfare" has been in use since 2001, when the conflict between the U.S. and Afghanistan began. The asymmetric nature of this war was immediately apparent, with a stark contrast in equipment, training, and capabilities between the opposing forces (Cvetković et al., 2019).

What distinguishes modern warfare from traditional armed conflicts is the emphasis on subduing the enemy without direct confrontation. This is achieved through special operations that maximize the use of advanced technology, specialized military units, terrorist activities, and organized crime (Rančić & Beriša, 2018).

Cognitive warfare, on the other hand, focuses on manipulating information and perception. As noted by Hung and Hung (2022), it is specifically aimed at controlling the brain by incorporating militarized neuroscience into various practices. It leverages disinformation, propaganda, and psychological tactics to influence public opinion and erode trust in institutions, transcending physical borders and deeply impacting societies.

Real-world examples highlight the urgency of addressing these threats. The 2017 NotPetya[1] cyberattack on Ukraine, Russia's interference[2] in the 2016 U.S. election, and proxy conflicts in Ukraine and Syria[3] all demonstrate the potency of these tactics. Additionally, the ongoing tensions between Morocco and Algeria show how hybrid and cognitive warfare are being deployed in regional disputes.

As we delve into this research overview, we aim to provide a deeper understanding of these evolving challenges and their impact on international security. By analyzing these

---

[1] **NotPetya attack:** In 2007, threat actors deploy a tool, with the purpose of encrypting data on victims' machines and rendering it unusable. The malware was spread through tax software that companies and individuals require for filing taxes in Ukraine.

[2] **Russian interference:** The Russian government used espionage to interfere in the 2016 United States elections with the goals of sabotaging the presidential campaign of Hillary Clinton, boosting the presidential campaign of Donald Trump, and increasing political and social discord in the United States.

[3] **Proxy conflicts** are wars where external powers indirectly participate by supporting local factions, providing military, financial, or political assistance to influence the outcome without direct involvement. These conflicts are driven by larger geopolitical interests. Examples include the **Ukraine conflict**, which began in 2014 with Russia's annexation of Crimea, and the **Syrian Civil War**, which started in 2011, with global powers like Russia, the U.S., and Iran backing different sides.

real-life examples, assessing international responses, and considering potential future scenarios, we seek to navigate the intricate domain of hybrid and cognitive warfare in an era characterized by complexity and uncertainty.

ANALYSIS OF RESEARCH FINDINGS

Hybrid warfare represents a dynamic and continually evolving form of conflict that challenges traditional definitions of war. It operates within the ambiguous spaces between peace and war, complicating the identification of responsible actors. Due to its multifaceted nature, effective responses to hybrid warfare require adaptability and a comprehensive approach.

Historically, armed conflicts have relied primarily on conventional military methods and techniques. The Military Encyclopedia defines war as "a complex and intense conflict driven by class, economic, and political contradictions, which, through the application of mass armed struggle, seeks to achieve the economic and political objectives of specific classes, states, or peoples" (Military Encyclopedia, 1974: 746).

The evolution of military strategies and insights from previous conflicts have demonstrated that objectives can also be pursued through non-military means. As warfare has transformed, so too have military doctrines. Hybrid warfare is a relatively recent concept, and its precise forms and methods remain to be fully delineated (Bjerregaard, 2011).

The concept of hybrid warfare is not universally accepted. For instance, the U.S. Department of Defense does not recognize hybrid warfare as a distinct form of modern conflict, questioning both its classification and the methods associated with it (Johnson, 2010).

Hybrid and cognitive warfare recognize no geographical boundaries and carry profound international implications. These threats have the potential to disrupt international relations, challenge alliances, and undermine the stability of regions. In an era of interconnectedness, the consequences of hybrid and cognitive warfare are far-reaching and extend beyond

individual nations. Therefore, international cooperation is paramount in addressing these multifaceted challenges.

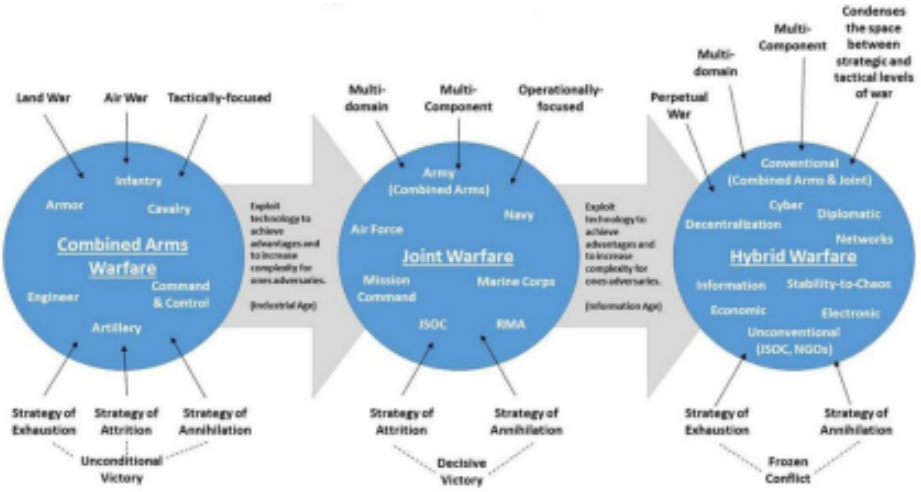

Figure 1: The evolution of hybrid warfare.[4]

NATO, as a cornerstone of collective defense, plays a pivotal role in addressing hybrid and cognitive warfare. The alliance's strength lies in its commitment to the principle of collective defense, enshrined in *Article 5* of the North Atlantic Treaty[5].

This commitment serves as a powerful deterrent to potential adversaries, as any attack against one member is considered an attack against all.

Cybersecurity is a critical component in countering hybrid and cognitive warfare. NATO has recognized the importance of cybersecurity and has established the NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE)[6] to enhance expertise and cooperation among member states. Robust cybersecurity measures are essential to protect critical infrastructure, sensitive information, and digital networks from cyberattacks.

NATO member states acknowledge the importance of public awareness and media literacy in countering cognitive warfare. Disinformation campaigns and psychological manipulation often target the public, and raising awareness is a crucial defense. Through information campaigns and education initiatives, NATO member states aim to bolster public resilience

[4] **Source**: Fox, A. (2017). Hybrid Warfare: the 21st Century Russian Way of Warfare

[5] **Article 5** provides that if a NATO Ally is the victim of an armed attack, each and every other member of the Alliance will consider this act of violence as an armed attack against all members and will take the actions it deems necessary to assist the Ally attacked.

[6] **The NATO Cooperative Cyber Defense Centre of Excellence** is a multinational and interdisciplinary hub of cyber defense expertise, the center enhances information security and cyber defense education, awareness, and training, provide cyber defense support for experimentation (including on-site) for experimentation, analyze the legal aspects of cyber defense.

against disinformation, ensuring that citizens can discern fact from fallacy and resist manipulation.

The multifaceted nature of hybrid and cognitive warfare demands international cooperation. NATO collaborates with various partners, including the *European Union* and other international organizations, to develop a unified response to these threats. Information sharing, joint response strategies, and collaborative efforts are essential in addressing these multifaceted challenges effectively. International cooperation strengthens the collective defense approach against hybrid and cognitive warfare.

RECOMMENDATIONS

Hybrid and cognitive warfare transcend national borders, demanding global responses. While the challenges are multifaceted, the international community has made significant strides in addressing these threats. In this section, we discuss the importance of international cooperation and offer recommendations, illustrated with examples, to effectively navigate the intricate domain of hybrid and cognitive warfare.

1. Strengthening cybersecurity through International Partnerships

Cyberattacks are a common component of hybrid warfare, often crippling critical infrastructure. International partnerships for cybersecurity, such as the Five Eyes Alliance[7](comprising the U.S., UK, Canada, Australia, and New Zealand), exemplify collaborative efforts to protect digital networks. These nations share cyber threat intelligence, bolstering collective defenses.

***Recommendation*:** Encourage the formation of international cybersecurity alliances to promote information sharing and collaborative strategies for mitigating cyber threats. Nations should seek opportunities to enhance cyber resilience through joint initiatives and knowledge sharing.

---

75 **The Five Eyes alliance**, consisting of the US, UK, Canada, Australia, and New Zealand, operates a cooperative intelligence network and employs various communication methods to monitor citizens in member countries.

2. Joint public awareness campaigns to counter disinformation

Disinformation campaigns are global in scope, targeting multiple countries simultaneously. In response, the European Union has undertaken campaigns to enhance media literacy, critical thinking, and resilience against disinformation. Initiatives like the EU's "EU vs Disinfo[8]illustrate international efforts to counter cognitive threats.

***Recommendation*:** Collaborate with international partners to launch joint public awareness campaigns. These campaigns should promote media literacy and educate citizens about the tactics employed in disinformation campaigns, ultimately reducing their impact on public opinion.

3. Global response frameworks for hybrid threats

Recognizing the urgency of hybrid threats, organizations like the United Nations have worked to develop response frameworks. The UN's Counter-Terrorism Committee Executive Directorate (CTED)[9] is an example of an entity focused on countering hybrid threats with a global perspective.

***Recommendation*:** Encourage the development of international response frameworks specific to hybrid and cognitive threats. These frameworks provide a structured approach to coordinate responses and share responsibilities, enabling rapid and unified reactions in the face of multifaceted challenges.

4. Coordinated crisis response to transnational threats

In the face of hybrid threats that transcend national boundaries, nations have increasingly coordinated their crisis response efforts. The collaboration between multiple countries during the WannaCry[10] ransomware attack and the international response to the Salisbury poisonings are examples of nations uniting against common threats.

Recommendation: Advocate for coordinated crisis response mechanisms on a global scale. These mechanisms should facilitate timely information sharing and coordinated actions

---

[8] Established in 2015, the task force's flagship project is EUvsDisinfo, a database of articles and media which the organization considers as providing false, distorted or partial information.

[9] **The Counter-Terrorism Committee Executive Directorate** (CTED) is a Special Political Mission which was established by UN Security Council resolution 1535 (2004) to assist the work of the CTC and coordinate the process of monitoring the implementation of resolution 1373 (2001).

[10] **WannaCry** is a ransomware worm that spread rapidly through across a number of computer networks in May of 2017. After infecting a Windows computer, it encrypts files on the PC's hard drive, making them impossible for users to access, then demands a ransom payment in bitcoin in order to decrypt them.24 août 2022

during transnational hybrid threat incidents. Such collaboration is pivotal in effectively managing crises that transcend individual nations.

CONCLUSION

In conclusion, hybrid and cognitive warfare are global challenges that necessitate international cooperation. The examples provided demonstrate the feasibility and effectiveness of such cooperation in addressing these multifaceted threats. By strengthening cybersecurity through international partnerships, launching joint public awareness campaigns, developing global response frameworks, and coordinating crisis responses, the global community can effectively navigate the intricate domain of hybrid and cognitive warfare. These recommendations serve as a roadmap for international actors to work together in safeguarding global security, trust, and democratic values in an era characterized by complexity and uncertainty.

REFERENCES

Achachi, R. (2023). *Au Maroc, prenons-nous au sérieux la guerre cognitive ?* Le 360 Français. Available at: https://fr.le360.ma/politique/au-maroc-prenons-nous-au-serieux-la-guerre-cognitive_LYCSGIJNE5HLHANHOGRYKGR6AM/

Bjerregaard, T. (2011). *Hybrid warfare: a military revolution or revolution in military affairs?* Swedish Armed Forces, B.M.S. Swedish National Defence College, Stockholm, Sweden.

Cvetković, N., Kovač, M., & Joksimović, B. (2019). *Pojam hibridnog rata.* Vojno delo, 71(7), 323–343.

Fox, A. (2017). *Hybrid Warfare: the 21st Century Russian Way of Warfare.* Leavenworth, KS: U.S. Army School for Advanced Military Studies.

Gartzke, E., & Lindsay, J. R. (2020). *Thermonuclear Cyberwar.* International Studies Quarterly, 64(3), 634-648.

Greenberg, A. (2018, August 22). *The untold story of NotPetya, the most devastating cyberattack in history.* WIRED. Available at: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

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, 7(4), ogac016.

Johnson, D. E. (2010). *Military Capabilities for Hybrid War: Insights from the Israel Defense Forces in Lebanon and Gaza.* USA.

Käihkö, I. (2021). *The evolution of hybrid warfare: Implications for strategy and the military profession.* USAWC Press. Available at: https://press.armywarcollege.edu/parameters/vol51/iss3/11/

Kozera, C. A., & Gürer, C. (2020). *Introduction to the Special Issue 'Proxy forces in modern warfare.'* Security and Defence Quarterly, 31(4), 11–15. https://doi.org/10.35467/sdq/132287

Nato (n.d.). *Joint declaration on EU-NATO cooperation by the president of the European Council, the president of the European Commission, and the secretary general of the North Atlantic Treaty Organization.* NATO. Available at: https://www.nato.int/cps/en/natohq/official_texts_156626.htm

Rančić, I., & Beriša, H. (2018). *Hibridni rat – mit ili stvarnost (Rekonceptualizacija hibridnog rata).* Vojno delo, 70(5), 255–271.

Watts, C., & Weisburd, A. (2016). *Trolling for Trump: How Russia Is Trying to Destroy Our Democracy.* Foreign Affairs.

Weissmann, M. (2019). *Hybrid warfare and hybrid threats today and tomorrow: Towards an analytical framework.* Journal on Baltic Security, 5(1), 17–26. doi:10.2478/jobs-2019-0002.