INTERNATIONAL CONFERENCE RCIC'25
Redefining Community in Intercultural Context
Brașov, 22-24 May, 2025

MILITARY ETHICS IN THE LIGHT OF COGNITIVE WARFARE

Ancuța RUSU

Security Systems Master's Programme, "Henri Coandă" Air Force Academy, Brașov, Romania

Abstract: *Hybrid warfare encompasses a broad spectrum of military and non-military tactics employed, in a coordinated manner, in order to destabilize and undermine adversaries. In the context of the Age of Hybridity, in the light of the use of new, unconventional operations, is the use of conventionally trained regular forces still effective? The answer is no. This paper explores part of the premises of the status rerum, along with the implications of the migration of the confrontational COG (Center of Gravity) from the physical and virtual domains, to the cognitive one. Taking into consideration the previously mentioned, the implementation of resilience training becomes increasingly interconnected to the field of military ethics. The goal of the paper is, therefore, to determine the correlation between advances in the field of cognitive research and the effectiveness of military resilience training, both from a doctrinal and an empirical point of view.*

Keywords*: hybrid warfare; ethics; cognitive warfare; resilience training*

1. INTRODUCTION

In the context of the Age of Hybridity, Cognitive Warfare, an important component of Hybrid Warfare, alongside its key components, such as Psychological Operations are difficult to monitor from an ethical point of view. Integrating the new and emerging military phenomena in the context of military ethics demands new ways of training, in order to achieve the desired level of preparedness of the military decision-making personnel. The advances in the field of cognitive research have made this possible. Through military resilience training, both physical and psychological toughness can be acquired

2. HYBRID WARFARE IN THE CONTEXT OF NATO ALLIED DOCTRINES

The Alliance doctrines emphasize the importance of rapid detection, effective deterrence and, if necessary, defense against hybrid attacks to safeguard member nations.

2.1 Key components. Hybrid warfare consists of multiple key components. Having realized the power that human perception holds in the decision-making process, it has been weaponized. As the great military strategist Sun Tzu once stated, "All war is based on deception". Therefore, planting a seed of specifically targeted information in one's mind can later grow to drastically influence the outcome of his process of thought and thus, his behavior. All of these have metamorphosed into disinformation and propaganda. According to (Hoffman, 2014), deliberately disseminating false or misleading information to influence public opinion, sow discord or manipulate perceptions, through media channels, social platforms or other communication means, can successfully serve an actor's strategies and objectives.

Moreover, taking into consideration that in the information age, most databases, military organization and communication systems and civil-military cooperation interfaces have migrated to the virtual domain, these have become critical infrastructure as well. Therefore, Cyber Attacks are an important aspect of hybrid warfare, being manifested through operations that target digital infrastructure in order to disrupt services, steal sensitive information or compromise critical systems.

Hybrid warfare, just like any other kind of warfare encompasses, inevitably, a political side and, can be manifested through political means just as well. Engaging in activities that influence the political processes of a nation, including influencing of the election process, supporting fringe political groups or undermining governmental institutions can create internal discord. There are also, more diplomatic ways of interference, such as economic pressure, using economic tools such as sanctions, trade restrictions or manipulation of

resources to coerce or weaken target nations. Last, but not least, it would be impossible to only focus on the overt side of hybrid warfare, when covert operations are being waged. This is where the ethics of new era military operations come in question. Conducting sabotage to damage or destroy critical infrastructure, such as power grids, communication networks or other societal functions, therefore instilling fear throughout the population, utilizing proxy forces, paramilitaries or insurgents to conduct military operations without direct attribution, can these be called covert operations or unethical demeanor? The line between the former and the latter is, unfortunately, not very clearly drawn.

2.2 Psychological Operations. The general context having been described, the particular one can come in sight. According to the Allied Joint Doctrine for Psychological Operations (AJP-3.10.1, 2014), PSYOPS are a key component of hybrid warfare, encompassing specialists and techniques used to manipulate the human perception in support of conventional operations.

The previously mentioned specialists can act in multiple ways: they can spread specifically designed and created narratives that exploit societal divisions, undermine trust in institutions, or create fear and uncertainty, they can use social media, traditional media or covert channels in order to shape the opinions of the target audience into fitting the given objectives, they can weaken the resolve of conventional military forces, government decision-making officials or the civilian population through misinformation, fake news or psychological intimidation or, moreover, they can act through covert means and exploit the cultural and political fault lines by amplifying existing societal conflicts, fueling protests, or creating artificial movement to destabilize a country from within. Trying to integrate all of these new and emerging concepts in the thinking systems of conventionally trained military leaders can prove to be difficult. Given the human nature: a tendency towards inertia and reluctance to change, it is hard to embrace new military phenomena and to develop the ways of proper training for the new era soldiers who need to be ready for these challenges

2.3 Cognitive Warfare. According to the Allied Joint Doctrine for Information Operations (AJP-10.1, 2023), there are three domains that belong to the information environment and where military operations can be lead. As enumerated on a temporal axis, according to their time of maximal importance, the physical, virtual and cognitive domains. The first two, interconnected as they are, are very well known together with the risks they imply. From the national and also from the military alliance point of view, the great majority of soldiers are trained as to recognize and manage threats that are specific to the physical and virtual domains or to correlations between the two. Thus, in the age of hybridity, threats related to the cognitive domain are more numerous and less easy to identify, so consequently, more dangerous. The training of all categories of military personnel lacks focus for the cognitive warfare aspects.

Hybrid warfare combines conventional and unconventional tactics. According to (Pripoae-Șerbănescu, 2023), if hybrid warfare will become the standard for confrontation in the future and the informational and psychological sides of hybridity will be the at the top of the threat spectrum, then Cognitive Warfare needs to become a must in matters of military studies in order to be able to fullfil the need to understand and respond to future security menaces. Having understood that, in the context of the previously mentioned, psychological influence can be technologically mediated, it is possible to agree on the fact that the Cognitive domain of confrontation is the one that crowns the pyramid of military confrontation domains.

Cognitive Warfare focuses on manipulating perceptions, influencing decision-making and undermining the adversary's psychological and cognitive processes. These effects can be acquired by directing specifically designed narratives of altered or manipulated information to the targets whose perceptions are aimed to be changed. Military decision-making personnel can most surely be integrated in the target audience category and be submitted to multiple attempts of manipulation or persuasion, aiming to influence the outcome of their thinking process. When analyzing the doctrinal perspective of the military alliance and the member states, it is obvious to conclude that most components of Cognitive Warfare and especially, of Psychological Operations are not exclusively directed to adversaries or potential adversaries, but also, to partner states and militaries. In the light of these facts, it is important that the security culture of soldiers encompasses knowledge of Cognitive Warfare, its place in Hybrid Warfare and threats that these new era operations imply.

2.4 Integrating new military phenomena in the context of military ethics. According to (Olsthoorn, 2010), military ethics is a branch of

applied ethics that governs the conduct of armed forces in war and peace. It defines the moral principles, values and standards that guide military personnel in their duties, ensuring that their actions are lawful, just and aligned with both national and international norms. However, if in the past the International Humanitarian Law and the Laws of Armed Conflict made ethics principles seem clear enough, in the age of hybridity, distinguishing between ethical and unethical seems to become more and more difficult.

Being the sixth NATO recognized domain of warfare, alongside land, sea, air, space and cyber, cognitive warfare is a requirement for winning modern conflicts, since control of territories is not the most important anymore. Disinformation and information manipulation, using fear, uncertainty and doubt in order to amplify societal divisions, social engineering, bot networks, perception management, strategic deception and decision disruption and paralysis are just some of the tactics used in the operations of Cognitive Warfare. The ethical character of the previously mentioned is, at best, questionable. The military ethics in the age of hybridity must become, accordingly, more flexible or the moral compass of those responsible of deciding when and whether it is ethical to lead such demeanors must be not so accurate nor very demanding. It is difficult to correlate the new components of hybrid warfare with the principles of military ethics. Hybrid warfare usually operates in the "gray zone", making it difficult to have a clear distinction between wartime and peacetime conduct. Moreover, by involving non-state actors, private companies and civilians, the military interactions surpass formal armed forces. While traditional military ethics focus on minimizing physical harm and suffering through the protection of non-combatants, another controversy arises: even if the attacks on public opinions, morale and societal trust do not cause direct physical harm, they can have devastating consequences. From another point of view, military ethics depend on clear attribution of actions for responsibility and accountability. However, hybrid attacks often use deniability through the employment of proxy forces, fake identities and anonymous cyberattacks. The line between military ethical and unethical demeanor is, consequently, thinner and blurrier than ever.

In order to attempt to integrate these new military phenomena in the context of military ethics, the most effective strategy that can be approached is developing countermeasures against cognitive warfare in order to avoid being manipulated by the adversaries, in terms of perceptions, emotions and decision-making.

2.5 Resilience training. Resilience is defined as the capacity to withstand or to recover quickly from difficulties. In a military context, resilience can no longer only refer to physical and virtual critical infrastructure. The cognitive domain must be included. Resilience training is a structured program designed to help individuals and groups develop mental, emotional and physical toughness in order to be able to more easily cooperate with stress, adversity and challenging situations. According to the Resilience Reference Curriculum (Lapsley & Vandier, 2025), military resilience training is designed to prepare soldiers for the psychological and physical demands of combat. Programs developed in the support of resilience training, such as U.S. Army's Master Resilience Training and NATO's comprehensive approach to resilience focus on enhancing mental toughness, strengthening effective leadership under pressure and maintaining operational effectiveness in crisis situations.

There are five levels of resilience: individual, community, organizational, national and multinational. The text of this paper focuses on resilience from an individual and organizational point of view. From a physical point of view, resilience concerns critical infrastructure, resources, networks, structures, or even how an institution is organized in terms of relationships, mechanisms and decision-making systems. The other element of resilience features psychological and emotional dimensions, concerning the determination and will to fight, civic duty, awareness and social cohesion.

The resilience process has four successive stages. The first is anticipation, where the individual has to observe, to identify and assess threats and prepare for them. The second one is managing, the stage where it is needed to effectively deal with the threat using support systems, resource allocation, coordination and information sharing. The third one is adapting, that comes after the crisis stage has passed and when the learning process can start, through cognitive understanding and behavioral shifts. The last one is recovering, where reflection can happen. Both the physical and psychological dimensions of resilience are closely interconnected, with each having the ability to influence the other. For instance, the state of physical infrastructure can affect mental well-being, just as psychological conditions can impact the use and perception of physical structures. Governments have a significant ability to shape the psychological resilience of their populations. However, while poor crisis management or a lack of transparency

can quickly erode trust and weaken psychological resilience, the process of building and sustaining trust and mental strength is far more complex and requires considerable time and effort.

According to the Master Resilience Training in the U.S. Army (J. Reivich *et al.*, 2011), the first operational and most important step in resilience training is building mental toughness by learning a series of skills that increase competencies. Soldiers learn to identify the link between activating events, their beliefs, and the resulting emotional and behavioral consequences. Through practical exercises, they recognize adaptive and counterproductive thought patterns. The program addresses explanatory styles and thinking traps that influence leadership and performance, helping soldiers detect cognitive errors like overgeneralization and develop strategies to correct them. It also focuses on recognizing deeply held beliefs ("icebergs") that can drive disproportionate emotional reactions, guiding soldiers in evaluating and adjusting these beliefs.

Energy management techniques, including controlled breathing and relaxation methods, are introduced to sustain resilience under stress. A structured problem-solving model teaches soldiers to overcome biases such as confirmation bias and to approach challenges systematically.

Training includes methods for minimizing catastrophic thinking by distinguishing between worst-case assumptions and realistic outcomes, and for challenging counterproductive thoughts in real time to maintain focus and performance. Finally, cultivating gratitude through daily reflection exercises reinforces positive emotions and strengthens interpersonal relationships.

The program emphasizes practical application of these skills to real-world military and personal situations, aiming to build long-term resilience and enhance overall psychological readiness.

All of these ways of developing resilience training programs for the military have been allowed to emerge by the advances in the cognitive research field. Modern developments in cognitive science have significantly deepened the understanding of how individuals react to stress, adapt to adversity, and maintain functional decision-making under extreme conditions. These findings have progressively shaped military resilience programs, enhancing both their theoretical foundation and practical methodologies to better prepare personnel for the psychological demands of contemporary operational environments.

One of the most impactful areas of research is in neuroscience. Studies on neuroplasticity have demonstrated that the human brain remains capable of restructuring itself even under conditions of intense stress. This insight has led to the development of training modules specifically aimed at reinforcing adaptive neural pathways. According to (Yanilov & Boe, 2020), military resilience programmes now incorporate exercises that target the cultivation of positive cognitive patterns, strengthen emotional regulation, and promote stress inoculation through repeated exposure to simulated adversities. By deliberately training the brain to adapt and recover, resilience programs build durable psychological defenses that enhance soldiers' performance under pressure.

In parallel, cognitive load theory has provided essential contributions to refining military training methods. Research has shown that excessive cognitive burden impairs decision-making and stress management, particularly in high-pressure situations. Consequently, military training curricula have been systematically adjusted to minimize unnecessary mental overload during instruction. Information delivery has been segmented, scenarios have been progressively structured to match cognitive capacities, and exercises have been designed to gradually build cognitive stamina. These adjustments ensure that personnel can process complex information more efficiently and maintain operational effectiveness even in cognitively taxing environments.

Behavioral psychology has also reshaped the approach to resilience training. Shifting from a reactive model, focused solely on coping with stress after the fact, modern programs now proactively cultivate traits such as perseverance, optimism, and emotional regulation. Frameworks like Growth Mindset and Grit Theory have been incorporated to encourage enduring motivation and adaptive emotional responses. As a result, behavioral interventions such as self-talk strategies, visualization techniques, and stress reframing exercises have become standard elements within resilience modules across many military forces. These techniques empower individuals to manage adversity proactively, rather than merely endure it.

From a doctrinal perspective, cognitive research has been increasingly integrated into formal military training frameworks, embedding psychological resilience as a critical capability. NATO's Comprehensive Approach to Resilience exemplifies this integration, emphasizing resilience as a multidimensional concept encompassing physical, societal, and cognitive domains. Cognitive resilience, in particular, is identified as vital for withstanding

disinformation campaigns, psychological manipulation, and other cognitive dimensions of hybrid warfare. Recognizing the centrality of the cognitive domain has led to the institutionalization of mental resilience within NATO's broader defense posture. Similarly, the evolution of Psychological Operations (PSYOPS) and emerging doctrines on Cognitive Warfare underscore the importance of mental resilience in safeguarding operational capabilities. These doctrines acknowledge that the psychological resilience of personnel is just as crucial as their physical protection. Advances in understanding vulnerabilities in information processing, as well as phenomena like emotional contagion, have informed the development of countermeasures designed to shield military personnel from influence operations. Targeted resilience-building initiatives now specifically address high-risk groups such as cyber operators, information analysts, and civil-military interaction teams, who are particularly exposed to cognitive threats.

Empirical evidence further supports the positive correlation between advances in cognitive research and the effectiveness of resilience training. Experimental findings, including neuroimaging studies, have revealed that individuals trained in resilience techniques exhibit different patterns of brain activation under stress, indicative of real neurological adaptation. These neurological changes correspond to improved emotional regulation, faster cognitive recovery after stress, and enhanced decision-making capabilities. Such findings validate the practical outcomes observed in operational environments, where personnel with resilience training demonstrate greater psychological durability and maintain performance even under extreme conditions.

3. CONCLUSIONS

In conclusion, In the context of the Age of Hybridity, cognitive dimensions of warfare have gained unprecedented importance, demanding a profound shift in military training, doctrines, and ethical frameworks. As hybrid threats continue to exploit vulnerabilities within the physical, virtual, and especially the cognitive domains, it becomes evident that traditional models of military preparedness are no longer sufficient. Psychological Operations and Cognitive Warfare, as integral components of hybrid conflict, have blurred the line between peace and war, adversary and ally, ethical and unethical conduct. Consequently, military resilience training must evolve, encompassing not only physical robustness but also psychological and cognitive strength. Advances in cognitive science have significantly contributed to the design of more sophisticated and effective resilience programs, equipping military personnel with the tools necessary to withstand, adapt, and recover from hybrid threats. Integrating an understanding of cognitive manipulation and fostering resilience at all organizational levels will be crucial for preserving decision-making integrity and ensuring operational effectiveness. In this new era, developing cognitive defenses is as vital as maintaining physical and cyber security. Future military leaders must be prepared not only to recognize and resist cognitive threats but also to navigate the increasingly complex ethical landscape of modern conflict.

This paper was made possible through the consultation of multiple NATO doctrinal publications, academic research on hybrid and cognitive warfare, and advances in cognitive and behavioral sciences. Special thanks are extended to those pioneering the integration of cognitive science into military resilience training, setting a new standard for the preparation of future armed forces. Their dedication to understanding the human dimension of conflict serves as a cornerstone for adapting military practices to the evolving nature of warfare in the 21st century.

BIBLIOGRAPHY

1. Hoffman, F.G. (2014). Hybrid warfare and challanges. In Th. Mahnken & J. Maiolo (eds.), *Strategic Studies. A Reader*. London: Routledge. 329-338.
2. Lapsley, A. & Vandier, P. (2025). *Resilience Reference Curriculum.* Brussels: NATO Headquarters.
3. NATO. (2007, October). *Allied Joint Doctrine for Psychological Opeations.* AJP-3.10.1(A). Brussels: NATO Standardization Agency.
4. NATO. (2023, January). *Allied Joint Doctrine for Information Operations* AJP-10.1. Brussels: NATO Standardization Agency.
5. Olsthoorn, P. (2010). *Military Ethics and Virtues.* London: Routledge.
6. Pripoae-Șerbănescu, C. (2023). Cognitive Warfare- Beyond Dominance, Manouvres and Information. *Romanian Military Thinking*. 4. 258-279.
7. Reivich, J.K.; Seligman, M.E.P. & McBride, S. (2011). Master Resilience Training in the U.S. Army. *American Psychologist*. 66(1). 25-34.

8. Yanilov, E., & Boe, O. (2020). *Combat mindset & fighting stress*. Tel Aviv: Dekel Publishing house and Meyer & Meyer Sport