

COGNITIVE RESILIENCE AS A CORE COMPETENCE IN THE MILITARY PROFESSION IN INFORMATION WARFARE ENVIRONMENTS

Ruslana Grosu¹
Cătălin-Victor Popescu²

Delivered: 26.6.2026.

Language: English

Corrected: 21.8.2026.

Type of paper: Review paper

Accepted: 27.8.2026.

DOI number: 10.5937/vojdelo2603107G

Abstract: The contemporary security environment, characterized by hybrid threats, information warfare, and large-scale cognitive influence operations, places increasing pressure on the decision-making capacities of military personnel and institutions. In this context, cognitive resilience emerges as a critical competence of the military profession, enabling military actors to maintain analytical clarity, resist cognitive manipulation, and sustain operational effectiveness under conditions of uncertainty and informational overload. This paper examines cognitive resilience as a multidimensional capability situated at the intersection of individual cognition, organizational culture, and systemic institutional adaptability. The study addresses the central research problem of how cognitive resilience can be conceptualized and operationalized as a strategic competence within modern military organizations exposed to persistent informational and psychological pressure.

The research aims to clarify the conceptual foundations of cognitive resilience and to identify its key functional components across individual, organizational, and systemic levels. The analysis is guided by the premise that strengthening cognitive resilience enhances the ability of military institutions to mitigate the effects of disinformation, perception management, and cognitive attacks in contemporary conflict environments. Methodologically, the study employs a qualitative conceptual analysis based on the review and synthesis of relevant literature from security studies, military sociology, and cognitive psychology.

The findings highlight the strategic importance of integrating cognitive resilience into military education, leadership development, and institutional learning processes in order to strengthen adaptive deci-

1 Armed Forces Military Academy „Alexandru cel Bun”, Chisinau, Republic of Moldova, e-mail: ruslana.grosu@gmail.com, <https://orcid.org/0000-0003-4871-737X>

2 Armed Forces Military Academy „Alexandru cel Bun”, Chisinau, Republic of Moldova, e-mail: popescuvictor546@gmail.com, <https://orcid.org/0009-0002-8485-1306>

sion-making and operational effectiveness in complex security environments.

Keywords: *cognitive resilience; military leadership; decision-making under stress; hybrid threats; information operations; mission command*

Introduction

Contemporary conflict environments are characterized by the rapid circulation of information and deliberate attempts to influence perception and decision-making processes. Under such conditions, the effectiveness of military actors depends not only on operational capabilities but also on their capacity to maintain cognitive clarity and disciplined judgment in information-saturated environments. Certain studies on hybrid threats and information manipulation emphasize that contemporary conflict targets both institutional structures and human cognition. Similarly, research on *cognitive warfare* highlights that modern strategic competition seeks to influence perception, trust, and decision-making processes. Such dynamics illustrate a broader transformation in the nature of contemporary conflict, where adversaries attempt to destabilize societies and institutions by shaping individuals' interpretation and responses to information.

In this context, the military profession must adapt by strengthening the cognitive capacities that enable personnel to interpret complex information environments and resist manipulation. *Cognitive resilience* therefore emerges as a critical professional competence that supports analytical clarity, situational awareness, and sound judgment under conditions of informational pressure and strategic ambiguity. The concept of *resilience* itself has evolved from a narrow understanding associated with recovery from disruption toward an interpretation emphasizing adaptation, learning, and the capacity to function effectively under uncertainty.

Within military organizations, *cognitive resilience* can be understood as the ability of personnel and institutions to preserve analytical discipline, maintain situational awareness, and make effective decisions in environments characterized by stress, ambiguity, and informational disruption. Military leaders and decision-makers are frequently required to process large volumes of information while simultaneously assessing threats, coordinating operations, and anticipating adversary behaviour. Importantly, *cognitive resilience* within the military profession should not be reduced to an individual psychological trait. Rather, it represents a professional capability embedded in training systems, leadership culture, and institutional learning processes. Modern armed forces must cultivate intellectual skills that allow personnel to evaluate information critically and resist attempts at manipulation. Educational initiatives aimed at strengthening analytical reasoning and media literacy can therefore play a decisive role in enhancing the cognitive preparedness of military personnel.

The significance of *cognitive resilience* also becomes clearer when considered within the broader framework of *national resilience*. Security scholars increasingly argue that *resilience* operates across multiple interconnected levels. This perspective

suggests that the *resilience* of military institutions cannot be separated from the wider *resilience* of the societies they protect.

Despite the increasing attention to *resilience* within security studies, existing research has largely focused either on *psychological resilience* at the individual level or on *societal resilience* within national security frameworks. At the same time, scholarship on hybrid threats and *cognitive warfare* highlights the vulnerability of decision-making processes in information-saturated environments. However, relatively limited attention has been devoted to understanding *cognitive resilience* as a professional competence of military personnel. The present study therefore addresses the insufficient conceptualization of *cognitive resilience* within the military profession and seeks to develop a framework explaining how this capability operates across different levels of the defence system.

The present study addresses this *conceptual gap* by examining *cognitive resilience* as a multidimensional capability embedded within professional military culture, organizational learning processes, and broader defence systems. Rather than treating *cognitive resilience* solely as an individual psychological trait, the paper conceptualizes it as a professional competence that operates across multiple interconnected levels of the defence system.

The *main objective* of the study is to develop a conceptual framework explaining how *cognitive resilience* contributes to maintaining effective decision-making within the military profession in complex information environments. Rather than focusing exclusively on the informational or psychological aspects of contemporary conflicts, the study examines how *cognitive resilience* contributes to the preservation of professional judgment and operational effectiveness. This emphasis is increasingly supported by the military psychology literature, which stresses that successful cognitive performance under stress carries “significant consequences” in military settings (Flood & Keegan, 2022).

More specifically, the research pursues *three interrelated objectives*. First, it clarifies the conceptual foundations of *cognitive resilience* within the broader literature on *resilience* and security governance. Second, it examines the relationship between *cognitive resilience* and the evolving nature of contemporary conflict, particularly in the context of hybrid threats and *cognitive warfare*. Moreover, overlaps and distinctions were identified between different strands of literature, especially where military and civilian conceptualizations diverge. This is particularly important in light of the “conceptual mismatches” identified between academic and NATO/military approaches (Deppe et al., 2024), including security governance, military cognition, hybrid threats, and human performance. Third, it proposes a conceptual model explaining how *cognitive resilience* operates across three interconnected levels of the defence system: the individual level of military cognition, the organizational level of institutional learning, and the systemic level of *national defence resilience*.

The study adopts a *qualitative conceptual research* design based on *literature analysis* and *theoretical synthesis*. The research relies on a structured review of interdisciplinary literature from security studies, military psychology, resilience theory, and

cognitive warfare research. Through comparative conceptual analysis, the study identifies the key dimensions of cognitive resilience and examines their relevance for military organizations operating in information-intensive environments. This approach is particularly necessary given the conceptual fragmentation that still characterizes the emerging field of *cognitive warfare* research, where a unified understanding has not yet been fully established (Deppe & Schaal, 2024; Deppe, Fotescu, & Schaal, 2024). By integrating insights from *resilience theory*, *cognitive security* research, and military studies, the paper contributes to the conceptual development of *cognitive resilience* as a core competence of the military profession. More specifically, the study advances the debate by proposing a *multilevel conceptual framework* that links individual cognitive capacities, organizational learning mechanisms, and systemic national resilience within a unified analytical perspective.

Cognitive pressures in contemporary conflict environments

The cognitive dimension of conflict has gained growing strategic relevance and military professionals are required to operate in environments characterized by information overload, ambiguity, and deliberate attempts to manipulate cognitive processes. As Cheatham et al. argue, *cognitive warfare* targets “gray matter” itself and may disrupt the capacity to know, judge, and respond effectively, while Flood and Keegan show that military personnel routinely perform complex cognitive operations under intense stress (Cheatham et al., 2024; Flood & Keegan, 2022). Recent studies on hybrid threats and information manipulation emphasize that contemporary conflict targets both institutional structures and human cognition. As Kaczmarek and Cholewińska (2024) note, hybrid strategies aim to undermine “national cohesion and security” through complex and ambiguous methods that operate below the threshold of conventional warfare (Kaczmarek & Cholewińska, 2024, p. 91). This observation highlights an essential shift in the nature of conflict: adversaries increasingly seek to destabilize societies and institutions by influencing perception, interpretation, and decision-making process.

Despite the growing academic attention to *resilience* in security studies, most existing research has focused either on *psychological resilience* at the individual level or on *societal resilience* within national security frameworks. Studies on hybrid threats and *cognitive warfare* emphasize the vulnerability of decision-making processes in information-saturated environments. While *cognitive resilience* forms the central analytical focus of this study, it is necessary to understand the strategic environment that makes such *resilience* indispensable. The contemporary security landscape is increasingly shaped by hybrid threats and information operations that seek to influence perception and behaviour rather than to achieve purely kinetic effects. Hybrid threats combine military, political, informational, cyber, and economic instruments to exploit vulnerabilities within societies and institutions. Such threats rarely aim at immediate

military victory; instead, they attempt to create confusion, erode trust, and weaken decision-making processes over time. Kaczmarek and Cholewińska (2024) emphasize that hybrid strategies exploit both institutional weaknesses and cognitive vulnerabilities in order to destabilize adversaries without engaging in open conflict. Within this framework, *information warfare* plays an important contextual role: the information environment has become a strategic domain in which narratives, perceptions, and interpretations can influence the outcome of conflicts. The rapid dissemination of information, combined with technological developments such as artificial intelligence and algorithmic amplification, has created conditions in which manipulation can occur at unprecedented speed and scale.

Mlejnková (2022) highlights that cyber-enabled psychological and information operations increasingly exploit “cognitive vulnerabilities” within societies and organizations (Mlejnková, 2022, p. 38). These vulnerabilities emerge from the inherent limitations of human cognition, including susceptibility to emotional stimuli, cognitive biases, and information overload. When exploited strategically, such vulnerabilities can distort perception and undermine effective decision-making. The informational environment therefore exerts continuous cognitive pressure on military actors. Commanders must interpret data originating from diverse sources while simultaneously assessing the reliability and strategic significance of that information. In such circumstances, maintaining situational awareness becomes a complex cognitive task. Mlejnková notes that modern conflict environments involve the interaction of “systems, information and people”, illustrating how technological and informational systems interact with human cognition to shape operational outcomes (Mlejnková, 2022, p. 39). Importantly, the effects of information operations extend beyond military organizations to society as a whole. Contemporary conflicts increasingly involve a “societal dimension of conflict”, in which public perception, social cohesion, and political trust become targets of strategic influence (Mlejnková, 2022, p. 45). In such environments, military institutions must operate within a broader ecosystem of *societal resilience*.

The interaction between *societal resilience* and *military resilience* has been widely recognized in security studies. Wigell, Mikkola, and Juntunen (2021) emphasize that countering hybrid threats requires a *whole-of-society approach* that integrates military, governmental, and societal actors (Wigell et al., 2021, p. V). Within such an approach, *resilience* is not limited to individual institutions but involves the protection of the “vital functions of society” as a whole (Wigell et al., 2021, p. 10). From this perspective, the military profession occupies an essential position within the broader architecture of *national resilience*. Military personnel must be capable of maintaining cognitive clarity even when confronted with manipulated information, ambiguous signals, and intense operational pressure. At the same time, military institutions must support these capacities through training, doctrine, and institutional learning mechanisms.

The concept of *cognitive resilience* thus serves as a bridge between individual cognition and systemic security: at the individual level, it enables military professionals to interpret information critically and resist manipulation; at the organizational level, it promotes institutional learning and analytical discipline; at the systemic level, it

contributes to the protection of societal cohesion and national security. In this sense, the contextual pressures generated by hybrid threats and *information warfare* do not replace traditional military challenges; rather, they expand the domain in which military professionalism must operate. The increasing importance of perception, interpretation, and narrative competition means that the integrity of cognitive processes has become an essential component of effectiveness.

Consequently, the central argument of this paper is that the military profession must treat *cognitive resilience* as a foundational competence. Hybrid threats and *information warfare* merely illustrate the conditions in which this competence becomes visible. The deeper issue concerns the capacity of military professionals and institutions to preserve rational judgment and disciplined analysis under conditions of uncertainty and cognitive pressure.

Conceptualizing cognitive resilience in the military profession on several levels

Cognitive resilience at the individual level

The *concept of resilience* has evolved significantly over the last decades, expanding from its initial application in psychology and disaster management to a broader analytical framework within security and strategic studies. In contemporary scholarship, *resilience* is increasingly understood as the capacity of individuals, organizations, and systems to anticipate, absorb, adapt to, and recover from disruptive events (Linkov & Trump, 2019; Normandin & Therrien, 2016). Yet this expansion has also produced conceptual diffusion, prompting calls for more integrated and context-sensitive *resilience* models (Šimelytė et al., 2025).

In this context, the military profession must adapt by strengthening cognitive capacities that enable personnel to interpret complex information environments. *Cognitive resilience* therefore becomes a key professional competence that allows military actors to maintain analytical clarity despite exposure to informational pressure and strategic ambiguity. The concept of *resilience* itself has evolved in recent decades from a narrow understanding of recovery from disruption toward a broader interpretation emphasizing adaptation and learning. In resilience research, *resilience* is increasingly understood as a “multidimensional approach” to coping with uncertainty and disruption (Bízík et al., 2022, p. 133).

Within the field of security studies, this conceptual evolution has led to growing interest in *cognitive resilience* as a key component of national and organizational security. *Cognitive resilience* refers to the capacity of individuals and institutions to maintain effective cognitive functioning in the face of informational disruption, psychological pressure, and strategic uncertainty. This capacity is particularly relevant in military environments where decision-makers must interpret complex operational realities un-

der conditions of ambiguity and time pressure. As Flood and Keegan (2022) note, *cognitive resilience* refers to “the degree to which cognitive functions can withstand” the effects of stress, and in military settings the need to preserve such functioning is especially acute because military personnel routinely perform cognitively demanding tasks under high stakes (Flood & Keegan, 2022, pp. 1-2).

The growing academic attention to *cognitive resilience* is closely linked to the emergence of hybrid threats and *cognitive warfare*. These forms of strategic competition aim to influence not only the physical domain of conflict but also the informational and psychological domains of confrontation. Research on *hybrid warfare* shows that contemporary conflict increasingly blends kinetic and non-kinetic measures and that battles now occur in the information space as well as in physical arenas (Splidsboel Hansen, 2017).

Similarly, the literature on *cognitive warfare* emphasizes the strategic importance of influencing human cognition itself. *Cognitive warfare* was defined as the “exploitation of human cognition and technology to disrupt, undermine, influence, or modify human decision-making”, while stressing that the concept is distinguished by its “distinct focus on cognitive effects” (Deppe & Schaal, 2024). Chifu (2025) considers that the “*cognitive warfare* thrives in political systems where trust in government is low, where social divisions divide people along deep ethnic, political, economic, social, or cultural lines, and where large segments of the population feel disconnected from the state and their fellow citizens” (Chifu et al., 2025, p. 66).

Within this strategic environment, *cognitive resilience* enables military actors to maintain analytical discipline and situational awareness despite exposure to misleading or conflicting information. It allows decision-makers to identify cognitive biases, critically evaluate information sources, and preserve rational judgment under stress. In research on *cognitive security*, it is highlighted¹³ that is the ability to generate cognition for efficient decision making in realtime by modelling human thought processes to detect cyber security attacks and develop defence strategies or, *cognitive security* is the ability to detect, characterize, and counter misinformation, disinformation, and other information-based harms and forms of malign influence among people. Resilience, as part of cognitive security, includes the structural context that protects humans from exposure to disinformation in the first place, as well as the ability to identify it, limit its spread, and mitigate its effects once exposed (Grahm & Taipalus, 2025). Cheatham et al. (2024) reinforce this by arguing that *cognitive warfare* “degrades the capacity to know, produce, or thwart knowledge”, which means that preserving the integrity of cognition is now operationally significant (Cheatham et al., 2024, p. 83).

The conceptual significance of *cognitive resilience* therefore lies in its *ability to bridge individual cognition and institutional effectiveness*. It represents a form of intellectual preparedness that complements physical readiness and technological capability. In modern security environments characterized by complexity and informational saturation, the preservation of cognitive integrity becomes a prerequisite for operational success. This is also consistent with broader research on AI-supported

systems, which argues that *cognitive resilience* should be defined as the capacity “to sustain attention, adapt to changing demands, and recover from stress-induced impairment” in high-stakes environments (Picchi, 2025).

At the *individual level*, *cognitive resilience* refers to the mental capabilities that enable military professionals to process information effectively and make sound decisions in challenging environments. Military personnel operate in conditions that frequently involve incomplete information, rapidly changing circumstances, and intense psychological pressure. Under such conditions, the ability to maintain clarity of thought and disciplined reasoning becomes essential. Several cognitive competencies contribute to individual *cognitive resilience*, including critical thinking, situational awareness, cognitive flexibility, emotional regulation, and resistance to cognitive bias. These competencies are increasingly discussed in the literature on *cognitive warfare* and decision-making under uncertainty (Cheatham et al., 2024; Nawaz, 2025). Nawaz shows that in the digital age information is “weaponized to manipulate public opinion, influence decision-making, and destabilize adversaries”, which makes bias awareness and critical evaluation indispensable (Nawaz, 2025, p. 21).

Critical thinking enables military personnel to evaluate information sources and detect inconsistencies in adversarial narratives. Situational awareness allows them to maintain an accurate understanding of operational environments despite the presence of conflicting signals. Cheatham et al. (2024) explicitly warn that saturation tactics, “sticky” information, and partial truths can prime cognition in ways that distort subsequent judgment, especially when they exploit confirmation bias and the brain’s tendency to accept disinformation under perceived threat (Cheatham et al., 2024, pp. 84-85).

Cognitive flexibility, meanwhile, refers to the ability to adapt mental models in response to new information. In dynamic operational contexts, rigid thinking can lead to strategic misinterpretation and operational failure. Flood and Keegan (2022) show that the effects of stress on cognition are mediated by appraisal, coping, and reappraisal processes, which means that *resilience* depends in part on the individual’s capacity to cognitively reframe and manage demanding situations (Flood & Keegan, 2022). Emotional regulation is equally important, as stress and emotional pressure can impair judgment and decision-making. Research on military cognition demonstrates that individuals who possess strong *cognitive resilience* are better equipped to manage uncertainty and complexity. Flood and Keegan note that in military settings cognitively demanding tasks are often carried out under intense stress and that promoting *cognitive resilience* is therefore a “high priority” (Flood & Keegan, 2022, p. 1).

Moreover, the concept of *cognitive readiness*, proposed by Grier (2012), has been linked to the ability to sustain performance under such conditions (Flood & Keegan, 2022). The development of such competencies requires systematic training and education. Military education systems increasingly emphasize analytical reasoning, problem-solving, and decision-making under uncertainty. Simulation exercises, scenario analysis, and war-gaming are commonly used to cultivate these skills. These training

approaches are consistent with the literature emphasizing the importance of *resilience-based education* in strengthening adaptive cognitive capacities (Lesenciuc et al., 2022). More specifically, Flood and Keegan (2022) review “methods of enhancing *cognitive resilience* in military personnel”, including mindfulness-based interventions and stress-inoculation approaches, and conclude that such methods can significantly improve working memory, attention, and stress tolerance in military populations (Flood & Keegan, 2022, p. 8).

Recent studies on *cognitive warfare* emphasize the importance of early cognitive preparation of military personnel as a means of strengthening *institutional resilience* against information manipulation. Bebbler (2025) argues that introducing inoculation-based training during the initial stages of military education can significantly enhance the *cognitive resilience* of armed forces. According to this approach, exposing recruits to simulated disinformation and influence operations during training helps develop a shared awareness of cognitive threats and prepares personnel to recognize manipulation attempts in operational environments.

Such training functions as a form of preventive cognitive defence, enabling military professionals to anticipate and resist attempts to distort perception or undermine institutional trust. By familiarizing recruits with the mechanisms of disinformation and psychological influence, military organizations can create a common cognitive framework that strengthens *collective resilience* across the force. In this sense, cognitive inoculation not only improves the analytical capabilities of individual servicemembers but also contributes to the broader operational effectiveness of military institutions operating in contested information environments (Bebbler, 2025). By exposing personnel to complex situations in controlled environments, training programs can strengthen *cognitive resilience* before individuals encounter real operational pressures. Cheatham et al. (2024) similarly argue that cognitive defence should become a “baseline skill set for every member of the joint force”, thereby positioning cognitive competence as part of the military profession itself rather than as a specialist add-on (Cheatham et al., 2024, p. 87).

Organizational dimensions of cognitive resilience

While individual cognitive abilities are very important, *cognitive resilience* cannot be fully understood without considering the role of *military institutions*, because the organizational structures, doctrines, and decision-making procedures significantly influence how information is processed and interpreted within military organizations. Within military organizations, *cognitive resilience* can be conceptualized as *the ability of personnel and institutions to preserve sound judgment, situational awareness, and analytical discipline under conditions of stress and informational disruption*. The importance of this capability becomes evident when considering the cognitive pressures faced by commanders and decision-makers operating in complex environments. Military leaders must process large volumes of information while simultaneously assess-

ing threats, coordinating operations, and anticipating adversary behaviour. The preservation of effective cognition under such circumstances requires more than technical training; it demands intellectual discipline and critical reflection. Delmonte emphasizes that maintaining operational effectiveness in contested information environments requires the development of “critical thinking” and the capacity for “overcoming biases” in decision-making processes (Delmonte, 2024, p. 4). These competencies are essential in preventing cognitive distortions that could compromise operational judgment.

Beyond individual cognitive abilities, *cognitive resilience* must also be understood as a professional capability embedded in training systems, leadership culture, and institutional learning processes. Modern armed forces must therefore cultivate intellectual skills that allow personnel to evaluate information critically and resist attempts at manipulation. Educational initiatives aimed at strengthening analytical reasoning and media literacy can play a decisive role in this process. In this regard, Delmonte highlights the importance of educational initiatives such as “media literacy programs” designed to support and “empower servicemembers” to recognize and resist manipulation (Delmonte, 2024, p. 5).

Certain research on *military resilience* suggests that the robustness of armed forces should be understood as a multidimensional phenomenon encompassing psychological, social, institutional, and national components (Divišová et al., 2023). These dimensions interact to shape the capacity of military organizations to maintain operational effectiveness under conditions of crisis, uncertainty, and external pressure. The effectiveness of the cognitive capabilities at individual level is closely linked to *institutional resilience*, understood as the perceived reliability and functional capacity of military organizations to support informed decision-making processes (Steinberg, 2009). When military institutions provide clear doctrine, structured decision-making procedures, and mechanisms for organizational learning, they reinforce the cognitive stability of their personnel.

Institutional resilience depends on the presence of mechanisms that facilitate learning, adaptation, and information filtering. Resilient institutions must be capable of absorbing shocks while maintaining functional stability and adapting their operational practices (Linkov & Palma-Oliveira, 2017). Yet in the cognitive domain this also means more than simple continuity: it requires institutions to actively reduce distortion and support sound collective judgment. Cheatham et al. note that defending the cognitive space of military personnel is “paramount” and that the US military still lacks a sufficiently tangible protective function for *cognitive security* inside the force (Cheatham et al., 2024, p. 85).

Military organizations that encourage analytical debate, critical reflection, and structured feedback are better equipped to maintain *cognitive resilience*. Conversely, rigid hierarchical cultures that discourage questioning may increase the risk of cognitive distortion and institutional blind spots. Organizational learning is therefore a central component of *cognitive resilience*. Through processes such as lessons-learned

programs and after-action reviews, military institutions can identify weaknesses in decision-making and adapt their practices.

Doctrinal frameworks also play an important role in shaping the cognitive environment within military organizations. In particular, the NATO Allied Command Transformation doctrine on mission command and national doctrinal documents such as the U.S. Army's ADP 6-0 (Headquarters, Department of the Army, 2019) emphasize decentralized decision-making and the empowerment of subordinate leaders as core principles of effective command. Similarly, NATO's Comprehensive Approach and resilience-oriented policy frameworks — including the NATO Baseline Requirements for National Resilience (NATO, 2016) — reflect doctrinal recognition of the cognitive and informational dimensions of contemporary conflict. Such approaches rely heavily on the cognitive competence of individual commanders, making *cognitive resilience* a prerequisite for effective leadership. This is particularly relevant in cognitively contested environments, where the problem is not only uncertainty but the deliberate shaping of uncertainty through manipulative information. Deppe and Schaal (2024) emphasize that *cognitive warfare* seeks to influence attitudes and behaviour by targeting cognition itself, often below the threshold of open conflict and through subtle, cumulative manipulations (Deppe & Schaal, 2024).

Additionally, *organizational resilience* requires the ability to manage information flows effectively. Military institutions must develop procedures that allow personnel to distinguish relevant information from noise. In environments characterized by information overload, the capacity to prioritize signals becomes essential for maintaining operational effectiveness. This insight is reinforced by literature on human-AI teaming, where Picchi (2025) shows that cognitive breakdowns such as attentional narrowing, working-memory collapse, and automation bias are not merely psychological concerns but operational vulnerabilities in high-stakes environments (Picchi, 2025).

Institutional culture also influences *resilience*, because the organizations that value intellectual curiosity and critical inquiry are more likely to adapt successfully to evolving security environments. By contrast, cultures that discourage dissent or alternative perspectives may inadvertently reinforce cognitive biases. Consequently, *cognitive resilience* at the organizational level emerges from the interaction between leadership practices, institutional learning mechanisms, and information management systems.

Systemic cognitive resilience and national defence

Beyond the individual and organizational levels, *cognitive resilience* also operates at the *systemic level* of national defence. At the same time, cognitive resilience is also influenced by the broader framework of *national resilience*, which encompasses societal cohesion, public trust in institutions, and shared national identity (Bízik et al., 2022). These factors shape the informational environment in which military actors operate and affect the credibility of narratives encountered during *information warfare* campaigns. Adversarial cognitive operations frequently seek to weaken precisely

these links between military institutions and society by undermining trust, legitimacy, and institutional credibility. Modern security environments involve complex interactions between military institutions, governmental agencies, and civil society. In this sense, *systemic resilience* provides the wider context within which military *cognitive resilience* is either strengthened or weakened.

The conceptual significance of *cognitive resilience* becomes even clearer when considered within the broader framework of *national resilience*. Security scholars increasingly emphasize that *resilience* functions at multiple interconnected levels. According to Wigell, Mikkola, and Juntunen, *resilience* should be analysed as a “nested” or layered attribute” that operates simultaneously at “societal, national and European levels” (Wigell et al., 2021, p. 19, p. 2). This layered understanding suggests that the *resilience* of military institutions cannot be separated from the broader *resilience* of the society they serve.

Whole-of-society approach to security emphasize that *resilience* must extend beyond military organizations. Recent resilience-oriented work argues that *resilience* should be treated as layered, socially embedded, and adaptive rather than as a purely technical attribute (Laine & Petersson, 2025). *Borderland* and *societal resilience* are increasingly understood as involving not only institutional capability but also informed, engaged, and connected communities (Laine & Petersson, 2025).

Systemic cognitive resilience therefore requires cooperation between military and civilian institutions. Strategic communication, media literacy programs, and psychological defence mechanisms can all contribute to strengthening societal resistance to manipulation. In this context, the term “psychological defence mechanisms” refers to the coordinated institutional measures and individual cognitive strategies designed to protect populations and organizations from the effects of disinformation, propaganda, and cognitive manipulation. At the institutional level, such mechanisms encompass structured counter-narrative programs, public awareness campaigns, and media literacy curricula; at the individual level, they involve cognitive techniques such as pre-bunking (inoculation against persuasion attempts), critical evaluation of information sources, and metacognitive awareness of one’s own cognitive biases (see Grahn & Taipalus, 2025; Bebbler, 2025). Countries exposed to hybrid threats have increasingly recognized the value of such measures. In this broader sense, *national defence resilience* should include not only military readiness and infrastructure robustness but also the protection of public interpretive capacity, social trust, and informed citizenship. *Systemic resilience* provides the strategic context in which individual and *organizational resilience* operate. A resilient national defence system supports military institutions by providing more stable information environments, stronger inter-institutional coordination, and a more resilient public sphere. In that sense, *cognitive resilience* is not reducible to the soldier or commander alone; it is partly conditioned by the health of the information ecosystem in which military institutions function.

The effectiveness of *cognitive resilience* therefore depends on the interaction between these levels. Weakness at one level can undermine *resilience* at others. For

example, even highly trained individuals may struggle to maintain cognitive clarity if institutional procedures generate excessive information overload. Conversely, strong institutional practices may be insufficient if individuals lack the cognitive skills necessary to interpret information critically. This is why the paper conceptualizes *cognitive resilience* as a professional competence distributed across the defence system rather than as a purely individual trait.

This perspective supports the *multilevel conceptual model* proposed in this paper, which links individual cognitive competence, *institutional resilience* mechanisms, and *systemic national defence resilience* within a unified analytical framework. Figure 1 provides a visual synthesis of the conceptual framework proposed in this study. While the text discusses the individual, organizational, and systemic dimensions of *cognitive resilience* separately, the figure illustrates how these levels interact within the broader architecture of the defence system.

By presenting *cognitive resilience* as a multilevel capability linking individual competencies, institutional learning processes, and national resilience structures, the model clarifies how these dimensions interact within contemporary defence systems. In doing so, it offers a structured perspective for understanding the role of cognition in modern military profession. This conceptual integration helps bridge previously fragmented discussions on *resilience*, *cognitive warfare*, and military profession, providing a coherent analytical basis for future empirical investigation.

SYSTEMIC COGNITIVE RESILIENCE (National Defence System)

- Whole-of-society resilience
- Strategic communication
- National information security
- Psychological defence
- Civil–military coordination





Figure 1. Multilevel conceptual model of cognitive resilience in the military profession

Conclusion

Cognitive resilience should be understood as a fundamental competence of the military profession in contemporary security environments shaped by hybrid threats and *information warfare*. Modern conflicts increasingly target the cognitive dimension of military activity by attempting to influence perception, distort interpretation, and disrupt decision-making processes. In such contexts, the preservation of analytical clarity and disciplined judgment becomes essential for maintaining operational effectiveness.

The study shows that *cognitive resilience* cannot be reduced to an individual psychological attribute. Instead, it represents a multidimensional professional capability

that emerges from the interaction between individual cognitive competencies, institutional practices, and the broader *resilience* of national defence systems. At the individual level, *cognitive resilience* involves critical thinking, cognitive flexibility, situational awareness, and the capacity to resist cognitive biases under conditions of stress and informational overload. At the organizational level, it depends on institutional mechanisms that support structured decision-making, analytical debate, and organizational learning. At the systemic level, *cognitive resilience* is closely linked to *societal resilience*, public trust in institutions, and the stability of the information environment in which military actors operate.

By conceptualizing *cognitive resilience* across these interconnected levels, the article highlights the need to integrate cognitive considerations more explicitly into military doctrine, professional military education, and institutional learning processes. Training programs that cultivate analytical reasoning, bias recognition, and decision-making under uncertainty can strengthen the capacity of military personnel to operate effectively in cognitively contested environments. At the same time, military institutions must develop organizational cultures and information-management practices that support sound collective judgment.

The conceptual framework proposed in this study contributes to the ongoing scholarly debate on the transformation of the military profession in the context of *cognitive warfare*. By linking individual cognition, *institutional resilience*, and systemic defence structures, the multilevel model clarifies how *cognitive resilience* functions as a bridging capability between professional military competence and the broader *resilience* of national security systems.

Future research should further explore how *cognitive resilience* can be operationalized and empirically assessed within military organizations. Comparative studies across different defence systems, as well as empirical investigations conducted through training environments and operational simulations, could provide valuable insights into the mechanisms that strengthen or weaken *cognitive resilience* in practice. Such research would contribute not only to theoretical refinement but also to the development of more resilient military institutions capable of operating effectively in increasingly complex and information-saturated security environments. In this sense, strengthening cognitive resilience may become one of the defining challenges of the military profession in the twenty-first century.

References

- [1] Bebbler, R. (2025). Information inoculation: Preparing US warfighters for cognitive war. Hudson Institute.
- [2] Bízik, V., Kosárová, D., Potočník, A., & Stojar, R. (2022). Hybrid interference: From the particular to a continuum, empirical test of the multi-dimensional concept of “hybrid”.

Obrana a Strategie (Defence and Strategy), 22(1), 75–88. <https://doi.org/10.3849/1802-7199.22.2022.01.075-088>

[3] Cheatham, M. J., Geyer, A. M., Nohle, P. A., & Vazquez, J. E. (2024). Cognitive warfare: The fight for gray matter in the digital gray zone. *Joint Force Quarterly*, 114, 83–91. <https://digitalcommons.ndu.edu/joint-force-quarterly/vol114/iss2/15/>

[4] Chifu, I. (2025). Conceptualization and epistemological evaluation: The cognitive warfare. In I. Chifu, E. Mârzac, & V. Konstantinova (Eds.), *Cognitive-Informational Warfare in the Romania - Republic of Moldova - Ukraine Trilateral* (pp. 47–72). RAO Bucharest.

[5] Delmonte, A. L. (2025). JCSP 51 – PCEMI n° 51 service paper étude militaire [Military study paper]. Department of National Defence.

[6] Deppe, C., Fotescu, A., & Schaal, G. S. (2024). The understanding of cognitive warfare in comparative perspective: Taking stock and bridging the gap to extant literatures. *Helmut Schmidt University/University of the Federal Armed Forces*.

[7] Deppe, C., & Schaal, G. S. (2024). Cognitive warfare: A conceptual analysis of the NATO ACT cognitive warfare exploratory concept. *Frontiers in Big Data*, 7, Article 1452129.

[8] Divišová, V., Frank, L., Bízík, V., & Novotný, A. (2023). A resilient soldier, a resilient state: A tool for measuring Czech Armed Forces' resilience against hybrid interference. *Obrana a Strategie (Defence and Strategy)*, 23(1), 173–191. <https://doi.org/10.3849/1802-7199.23.2023.01.173-191>

[9] Flood, A., & Keegan, R. J. (2022). Cognitive resilience to psychological stress in military personnel. *Frontiers in Psychology*, 13, Article 809003. <https://doi.org/10.3389/fpsyg.2022.809003>

[10] Grahn, H., & Taipalus, T. (2025). Defining comprehensive cognitive security in the digital era: Literature review and concept analysis. *Journal of Information Warfare*, 24(2), 39–59. <https://www.jinfowar.com/journal/volume-24-issue-2/defining-comprehensive-cognitive-security-digital-era-literature-review-concept-analysis>

[11] Headquarters, Department of the Army. (2019). ADP 6-0: Mission command: Command and control of Army forces. U.S. Army.

[12] Kaczmarek, K., & Cholewińska, D. (2024). Security and hybrid threats. *Przegląd Nauk o Obronności*, 20, 91–100. <https://doi.org/10.37055/pno/208458>

[13] Kosárová, D., Bízík, V., & Potočná, A. (2024). Cognitive resilience: Assessing critical factors in military personnel. *Obrana a Strategie (Defence and Strategy)*, 24(2), 133–156. <https://doi.org/10.3849/1802-7199.24.2024.02.133-156>

[14] Laine, J. P., & Petersson, B. (2025). Resilience as adaptive deterrence in an era of strategic uncertainty. In J. P. Laine & B. Petersson (Eds.), *Resilience as deterrence: Towards a comprehensive security panorama* (pp. 1–15). IOS Press.

[15] Lesenciuc, A., Nagy, D., & Lesenciuc, S. (2022). Societal resilience: Between resilience through education and resilience through war. *International Conference RCIC'22 „Redefining Community in Intercultural Context”*, Braşov, Romania, 25–32.

[16] Linkov, I., & Palma-Oliveira, J. M. (2017). Infrastructure resilience assessment, management and governance. In *Resilience and risk* (pp. 147–187). Springer.

- [17] Linkov, I., & Trump, B. D. (2019). Resilience and governance. In *The science and practice of resilience* (pp. 35–52). Springer.
- [18] Mlejnková, P. (2022). Issues of resilience to cyber-enabled psychological and information operations. *Vojenské Rozhledy*, 31(1), 38–50.
- [19] NATO. (2016). Baseline requirements for national resilience. NATO Allied Command Transformation.
- [20] Nawaz, F. (2025). Psychological warfare in the digital age: Strategies, impacts, and countermeasures. *Journal of Future Building*, 2(1), 21–30.
- [21] Normandin, J.-M., & Therrien, M.-C. (2016). Resilience factors reconciled with complexity: The dynamics of order and disorder. *Journal of Contingencies and Crisis Management*, 24(2), 107–118.
- [22] Picchi, A. (2025). Designing for cognitive resilience in human-AI teams: A neuroadaptive approach to operational integrity and decision superiority. ResearchGate. https://www.researchgate.net/publication/392933806_Designing_for_Cognitive_Resilience_in_Human-AI_Teams_A_Neuroadaptive_Approach_to_Operational_Integrity_and_Decision_Superiority
- [23] Šimelytė, A., Vveinhardt, J., & Deikus, M. (2025). Socioeconomic resilience in the context of sustainability: A comparison of the Nordic and Baltic states. *Management Theory and Studies for Rural Business and Infrastructure Development*, 47(2), 187–204. <https://doi.org/10.15544/mts.2025.15>
- [24] Splidsboel Hansen, F. (2017). Russian hybrid warfare: A study of disinformation. Danish Institute for International Studies.
- [25] Steinberg, P. F. (2009). Institutional resilience amid political change: The case of biodiversity conservation. *Global Environmental Politics*, 9(3), 61–81. <https://doi.org/10.1162/glep.2009.9.3.61>
- [26] Wigell, M., Mikkola, H., & Juntunen, T. (2021). Best practices in the whole-of-society approach in countering hybrid threats. European Parliament..

Summary

The contemporary security environment is defined by the growing prevalence of hybrid threats, information warfare, and large-scale cognitive influence operations that place unprecedented pressure on the decision-making capacities of military personnel. In this context, cognitive resilience has emerged as a critical professional competence for the military profession, enabling military actors to preserve situational awareness, resist informational distortion, and sustain effective judgment under conditions of uncertainty and psychological pressure. This paper examines cognitive resilience as a multidimensional professional competence situated at the intersection of individual cognition, organizational culture, and systemic institutional adaptability.

The central research problem addressed is how cognitive resilience can be conceptualized and operationalized as a strategic competence within modern military organizations persistently exposed to informational and psychological pressure. The study adopts a qualitative conceptual research design based on a structured review of interdisciplinary literature drawn from security studies, military psychology, resilience theory, and cognitive warfare research.

The analysis is structured around three interconnected levels of cognitive resilience. At the individual level, cognitive resilience encompasses the mental capabilities that enable military professionals to process information effectively, maintain situational awareness, and make sound decisions in challenging environments. Key competencies include critical thinking, cognitive flexibility, emotional regulation, and resistance to cognitive bias, which are capacities that can be developed through systematic training, simulation exercises, and inoculation-based educational approaches. At the organizational level, cognitive resilience is conceptualized as an institutional capability embedded in training systems, leadership culture, and organizational learning processes. Doctrinal frameworks, including mission command principles as articulated in NATO doctrine and ADP 6-0, play a significant role in shaping the cognitive environment by promoting decentralized decision-making. At the systemic level, cognitive resilience is understood as a component of broader national defence resilience, which includes societal cohesion, public trust in institutions, and the integrity of the information ecosystem.

The paper also addresses the systemic dimension by examining how whole-of-society approaches contribute to the protection of public interpretive capacity. In this context, "psychological defence mechanisms" refer to the coordinated institutional measures and individual cognitive strategies designed to shield populations from disinformation, propaganda, and cognitive manipulation, operating through counter-narrative programs, media literacy curricula, pre-bunking techniques, and metacognitive awareness of cognitive biases.

The principal contribution of this study is a multilevel conceptual framework that links individual cognitive competencies, organizational learning mechanisms, and systemic national resilience structures within a unified analytical perspective. The framework clarifies how the three levels interact: individual cognitive capabilities depend on institutional support structures; organizational resilience requires cognitively prepared personnel; and systemic resilience is partly conditioned by the health of the information ecosystem in which military institutions function.

The findings highlight the strategic importance of integrating cognitive resilience into military education, leadership development, and institutional learning processes. Future research should explore how cognitive resilience can be operationalized and empirically assessed within military organizations, including through comparative studies across defence systems and empirical investigations in training environments. Strengthening cognitive resilience may prove to be one of the defining professional challenges of the military vocation in the twenty-first century.

Keywords: cognitive resilience; military leadership; decision-making under stress; hybrid threats; information operations; mission command

© 2026 The Authors. Published by Vojno delo (<http://www.vojnodelo.mod.gov.rs>). This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution license (<http://creativecommons.org/licenses/by/4.0/>).



