DOI: 10.53477/3045-2309-26-05

COGNITIVE RESILIENCE AS A STRATEGIC ASSET IN CONTEMPORARY WARFARE: THEORETICAL FOUNDATIONS AND SECURITY IMPLICATIONS

Ruslana GROSU, PhD,
Associate Professor, Armed Forces Military Academy "Alexandru cel Bun",
Chisinau, Republic of Moldova,
E-mail address: ruslana.grosu@gmail.com

Cătălin-Victor POPESCU,
PhD Student, Armed Forces Military Academy "Alexandru cel Bun",
Chisinau, Republic of Moldova,
E-mail address: popescuvictor546@gmail.com

Abstract*: Contemporary warfare is increasingly shaped by cognitive dynamics that influence perception, decision-making, and strategic behaviour across state and non-state actors. While traditional security studies have emphasised kinetic capabilities and material resources, less attention has been paid to cognitive resilience as a strategic asset in modern conflict environments. This paper advances a conceptual and analytical framework that positions cognitive resilience as a core component of contemporary security and warfare.*

Building on interdisciplinary literature, the paper clarifies the concept of cognitive resilience and differentiates it from adjacent constructs. The analysis situates cognitive resilience within contemporary warfare environments characterised by hybrid conflict and prolonged strategic competition. It demonstrates how cognitive vulnerabilities such as rigidity, cognitive overload, and susceptibility to disinformation can undermine strategic effectiveness even in technologically advanced actors.

The paper further conceptualises cognitive resilience as a strategic asset by linking it to security culture and leadership, proposing an analytical framework outlining key dimensions of cognitive resilience and their relevance for defence policy, military education, and security governance. By doing so, the paper contributes to ongoing debates on cognitive security and offers a theoretically grounded foundation for future empirical and comparative research. Overall, the study positions cognitive resilience as a critical yet under-theorised pillar of international security in contemporary warfare contexts across evolving conflict domains.

Keywords*: cognitive resilience; cognitive security; hybrid warfare; information warfare; strategic adaptability; security culture.*

Introduction

Cognitive resilience refers to the capacity to preserve essential cognitive functions, such as perception, attention, situational assessment, reasoning, and decision-making, under conditions of physiological strain, psychological pressure, or environmental disruption. Initially developed within psychology, neuroscience, and mental health research, the concept has undergone substantial theoretical refinement. In line with clinical and neuropsychological literature, *cognitive resilience* is understood as the capacity to sustain better-than-expected cognitive functioning despite the presence of adverse factors, reflecting an individual's ability to maintain cognitive performance under conditions of vulnerability or decline (Elman et al. 2022).

Early interpretations framed resilience as a relatively stable individual trait; contemporary approaches, however, conceptualize it as a dynamic and adaptive process emerging from the interaction of genetic predispositions, environmental conditions, and individual cognitive-emotional resources, which can be developed and strengthened over time. *Cognitive resilience* is defined as the capacity of individuals and systems to sustain adaptive reasoning, tolerate ambiguity, resist manipulation, and maintain *strategic coherence* under conditions of cognitive stress, uncertainty, and information saturation. These capacities are no longer merely individual traits, but collective and institutional resources with direct strategic value.

The significance of *cognitive resilience* has been well documented in relation to mental health outcomes, cognitive aging, and educational performance, where it is associated with sustained functioning and adaptive capacity in the face of adversity (Parsons, Kruijt & Fox 2016, 296-299). Foundational research conducted in the mid-twentieth century marked a turning point in *resilience* studies, as scholars began to move beyond deficit-oriented models focused on vulnerability and pathology. Influential contributions redirected attention toward strengths-based perspectives, emphasising positive adaptation, learning, and proactive coping mechanisms. This shift laid the groundwork for contemporary understandings of *resilience* as a continuum shaped by both protective and risk factors, including social support networks, emotional regulation abilities, and biological predispositions.

Despite this expanding body of research, persistent challenges remain regarding the operationalisation and measurement of *cognitive resilience*. The absence of standardised assessment frameworks and the coexistence of diverse conceptualisations continue to generate ambiguity, particularly when the concept is applied beyond individual-level analysis. These limitations become especially salient when *cognitive resilience* is invoked in contexts characterised by high uncertainty, strategic competition, and deliberate attempts to influence cognition and behaviour.

In parallel with these conceptual developments, the contemporary security environment has undergone a profound transformation. The proliferation of hybrid threats, information warfare, and digitally mediated influence operations, often enhanced by artificial intelligence, has shifted the locus of strategic competition toward the cognitive domain. Rather than targeting material capabilities alone, adversaries increasingly seek to disrupt perception, distort situational awareness, fragment judgment, and undermine decision-making processes at individual, institutional, and societal levels. Decision-makers, military personnel, and civilian populations alike are exposed to sustained cognitive pressure aimed at eroding coherence, trust, and adaptive capacity.

Research Problem

Although recent literature increasingly acknowledges the importance of *cognitive resilience*, the concept remains fragmented across psychological, organisational, and security-oriented approaches. *Cognitive resilience* is often treated either as an individual psychological trait or as a loosely defined societal capacity, while its strategic relevance in contemporary warfare remains insufficiently conceptualised. In particular, there is a lack of integrated theoretical frameworks explaining how and under what conditions *cognitive resilience* can function as a *strategic asset*, capable of mitigating *cognitive warfare* effects and supporting *adaptive deterrence* and decision security.

The core research problem addressed in this study therefore lies in the insufficient conceptualisation of *cognitive resilience* as a governable strategic resource, situated at the intersection of behavioural sciences, security studies, organisational governance, and contemporary warfare. The present study seeks to address this gap by clarifying the conceptual foundations of *cognitive resilience* and articulating its relationship to *cognitive security*, decision integrity, and strategic performance in modern conflict environments.

Research Objectives

The *general objective* consists of analysis and conceptualising of *cognitive resilience* as a *strategic asset* in contemporary warfare by integrating insights from behavioural sciences, security studies, resilience governance, and *cognitive warfare* literature.

Several *specific objectives* follow: to provide conceptual clarification of *cognitive resilience* by distinguishing it from related concepts such as general *psychological resilience*, information security, and *cyber resilience*; to identify and analyse active and passive cognitive stressors relevant to contemporary warfare and assess their impact on individual and organisational cognitive functioning; to examine the relationship between *cognitive resilience* and *cognitive security*, with a particular focus on organisational and institutional dimensions; to evaluate the role of *cognitive resilience* in *adaptive deterrence*, decision coherence, and the reduction of adversarial strategic advantage. The study develops an integrated theoretical framework enabling the operationalisation of *cognitive resilience* in military, institutional, and societal contexts.

Methodology

This study adopts a qualitative, theory-driven research design grounded in conceptual analysis and integrative literature review. Given the exploratory and foundational nature of the research question, namely, the conceptualisation of *cognitive resilience* as a *strategic asset* in contemporary warfare, the methodology prioritises theoretical coherence, analytical rigour, and interdisciplinary synthesis rather than empirical testing. The research is structured as a conceptual-analytical study, drawing on established approaches in security studies and *resilience* research that aim to clarify concepts, integrate fragmented literature, and generate theoretically grounded frameworks applicable to complex security environments.

1. Literature Review

The literature employed in this study was selected based on conceptual relevance, academic rigour, and strategic applicability, reflecting the inherently interdisciplinary nature of *cognitive resilience* as a research area. The reviewed works are structured into five interrelated problem blocks, each contributing a distinct analytical dimension to the study.

The first block, which concerns *cognitive warfare and the transformation of the security environment*, addresses the conceptual emergence of *cognitive warfare* as a defining feature of contemporary conflict. Key authors emphasise that modern adversaries increasingly target perception, judgment, and decision-making rather than exclusively physical assets. Foundational contributions include military and policy-oriented analyses that frame *cognitive warfare* as operating within the digital gray zone and aiming at cognitive effects rather than kinetic outcomes (Cheatham et al. 2024; Ariton 2025). A comparative and NATO-aligned conceptual work stresses the need to delimit *cognitive warfare* analytically, warning against conceptual overstretch and terminological inflation (Deppe & Schaal 2024; Deppe, Fotescu & Schaal 2024). Claverie and Du Cluzel (2022) do not provide an explicit definition of *cognitive resilience*; instead, *resilience* is implicitly framed as a defensive and preventative capacity within *cognitive warfare*, associated with the protection of perception, judgment, and decision-making processes at individual and societal levels (Claverie & Du Cluzel 2022).

The second block, which elucidates *cognitive security* and the protection of cognitive assets, focuses on the transition from describing cognitive threats to defining what must be protected, namely cognitive assets such as attention, judgment, trust, and decision-making capacity.

Cognitive security scholarship reframes the human mind as a security-relevant asset exposed to both adversarial and systemic degradation (Ask et al. 2025). Architecture-informed and human-factors approaches advance this perspective by proposing design and governance mechanisms that protect cognition without compromising democratic norms (Doherty 2023; Tossell et al. 2025).

The block referring to *resilience* theory, governance, and *strategic deterrence* situates *cognitive resilience* within broader debates on *resilience* as a *security* concept, emphasising both its analytical value and its political implications. Critical security scholarship highlights that *resilience* is not neutral, warning against its performative and responsibilising effects (Brassett & Vaughan-Williams 2015). Governance-oriented literature reframes *resilience* as an institutional capability requiring coordination, accountability, and policy design (Linkov & Trump 2019; Heinimann & Hatfield 2017). Strategic analyses further conceptualise *resilience* as *adaptive deterrence*, directly linking it to strategic competition and security outcomes (Laine & Petersson 2025; Ziehr & Merkt 2024).

The block about disinformation, psychological operations, and cognitive stressors examines *cognitive resilience* in relation to disinformation, psychological operations, and influence campaigns, which represent key operational tools of *cognitive warfare*. Empirical studies on *resilience* to disinformation identify cognitive and social correlates that shape susceptibility and resistance (Mider & Żółtowski 2025). Educational and diagnostic interventions demonstrate that *cognitive resilience* can be deliberately cultivated at societal and organisational levels (Molek-Kozakowska 2024; Bebber 2025). Analyses of cyber-enabled psychological operations emphasize the convergence of informational and cognitive attack vectors (Mlejňková 2022; Meghraoui & Belkhamza 2025).

The final block, which approaches organisational, military, and whole-of-society perspectives, expands *cognitive resilience* beyond individual and unit-level considerations toward organisational, national, and whole-of-society frameworks. Military-focused research provides rare attempts to assess *cognitive resilience* among personnel and link it to operational effectiveness (Kosárová, Bízík, & Potočňák 2024). European and regional security analyses highlight the role of *cognitive resilience* in defence challenges and societal preparedness (Senčar 2021; Hansen 2017). Policy-oriented and institutional reports emphasise cross-sector coordination and societal cohesion as essential components of *resilience* against hybrid threats (Wigell, Mikkola, & Juntunen 2021; Teperik et al. 2018; Semenenko et al. 2025).

The selection of 45 sources reflects a deliberate methodological choice to combine theoretical depth with strategic relevance. Behavioural science literature provides the foundational understanding of *resilience* and cognitive adaptation, while security and defence studies contextualise the *cognitive resilience* within contemporary warfare. Governance and organisational scholarship enable the treatment of *cognitive resilience* as a managed institutional capability, and recent work on AI, disinformation, and hybrid threats situates the analysis in the current operational environment. Together, these sources support a coherent argument that *cognitive resilience* constitutes a strategic asset only when it is governed, designed, and operationalised across individual, organisational, and societal levels, thereby preserving decision integrity and constraining adversarial influence in contemporary warfare.

2. Conceptualizing Cognitive Resilience in the Context of Contemporary Warfare

Cognitive resilience originates in *resilience* research within the behavioural sciences, where *resilience* has traditionally been understood as a dynamic process involving exposure to adversity and the capacity for positive adaptation in response to that adversity (Luthar & Cicchetti 2000). Early formulations positioned *resilience* primarily within trait psychology and individual coping capacities, emphasizing psychological robustness and recovery following stress or disruption. Within this tradition, *cognitive resilience* was defined as the "capacity to overcome the negative effects of setbacks and associated stress on cognitive function and performance" (Staal et al. 2008, p. 260). While analytically useful, such definitions largely reflect individual-level adaptation and remain insufficient for explaining *resilience* in strategically contested environments.

More recent research has extended *resilience* theory beyond individual traits toward systemic, organisational, and security-oriented interpretations. The relationship between *cognitive resilience* and military personnel has been examined through a performance-oriented lens, highlighting how the

ability to maintain cognitive functioning under stress, fatigue, and operational pressure is critical for sustaining effectiveness in demanding military environments (Staal et al. 2008, as discussed in Flood & Keegan 2022, p. 8). When cognition becomes a target, *resilience* becomes a security capability.

This evolution is particularly relevant in the context of contemporary warfare, where cognitive processes themselves such as perception, judgment, attention, sensemaking, and decision-making have become deliberate targets of adversarial action. From this perspective, *cognitive resilience* must be understood not merely as psychological endurance, but as a security-relevant capability that safeguards cognitive functioning under conditions of persistent pressure, uncertainty, and hostile influence. *Cognitive resilience*, which is the ability of systems and societies to resist manipulative exploitation and the distortion of perception, is a fundamental issue to be considered in the field of cybersecurity (Bierecki, Gaie, Karpiuk & Langlois-Berthelo 2025, pp. 139-140).

Within the emerging field of *cognitive security*, stressors affecting *cognitive resilience* are conceptualised as both *active* and *passive*. *Active stressors* arise from intentional adversarial efforts aimed at accessing, degrading, or manipulating cognitive assets, including individuals, groups, and decision-making structures (Masakowski & Blatny 2022). Such stressors are characteristic of *cognitive warfare*, disinformation campaigns, psychological operations, and influence strategies designed to distort judgment, erode trust, or disrupt strategic coherence. Building on NATO conceptualisations of *cognitive warfare*, *active stressors* can be understood as intentional adversarial efforts aimed at accessing, degrading, or manipulating cognitive assets, ranging from individual cognition to collective decision-making structures (Claverie & Du Cluzel 2022). In contrast, *passive stressors* refer to the natural and cumulative degradation of cognitive performance over time, independent of direct adversarial intent. These include prolonged workload, cognitive fatigue, stress accumulation, information overload, and environmental pressures that reduce attentional control and decision accuracy. Although Vrijkotte et al. (2016) do not explicitly conceptualise *passive stressors*, their analysis provides strong empirical evidence for cumulative, non-adversarial stressors that progressively degrade cognitive performance through sustained workload, fatigue, sleep deprivation, and environmental pressure (Vrijkotte et al. 2016). Importantly, *passive stressors* do not merely coexist with active threats; rather, they amplify vulnerability to hostile cognitive influence. Extended sustained operational tempo, diminished motivation to engage in security-enhancing behaviours, or heightened emotional strain can significantly weaken cognitive acuity and increase susceptibility to manipulation. *Cognitive resilience* therefore emerges at the intersection of internal cognitive resource management and external threat exploitation.

The maintenance of *cognitive resilience* over time depends on the balance between *passive coping* and *active engagement* with these stressors. *Passive coping strategies*, such as avoidance, or emotional numbing, may offer short-term relief but ultimately erode *cognitive resilience* and impair decision-making capacity. In contrast, *active coping* involves the deliberate application of cognitive strategies, training, and organizational measures that sustain cognitive performance and adaptive capacity under pressure. From a *cognitive security* perspective, *active engagement* is not an individual responsibility alone but an organisational obligation, requiring deliberate design, coordination, and governance.

In this respect, *cognitive resilience* parallels the evolution of *cyber resilience* as an organisational state rather than a purely technical or individual attribute. *Cognitive resilience* entails a holistic and comprehensive response to cognitive threats, in which individuals at all levels of an organisation or institution possess a shared understanding of the threat landscape and their role within it (Ask et al. 2024b). Procedures for anticipating, absorbing, and adapting to harmful situations must be embedded structurally, reflecting the expectation that unexpected and disruptive cognitive challenges will inevitably occur. *Resilience*, therefore, is not the absence of vulnerability, but the capacity to function, decide, and adapt despite it.

Within contemporary warfare, this organisational framing has critical strategic implications. Individuals constitute cognitive assets whose degradation can generate cascading effects across units, organisations, and even national systems. Targeting a single individual through biological,

psychological, or informational means may significantly impair collective decision-making if that individual occupies a strategic or operationally central role. Similarly, coordinated influence operations targeting multiple members of a subgroup or society can generate social incoherence, erode institutional trust, and weaken *national cognitive security*, thereby reducing a state's capacity to respond effectively to subsequent adversarial actions.

Accordingly, *cognitive resilience* must be conceptualised as *a strategic asset*: a collective, governed, and deliberately cultivated capability that protects the cognitive foundations of military effectiveness, societal cohesion, and strategic decision-making. In contemporary warfare, characterised by hybrid threats, persistent competition, and AI-enabled influence, *cognitive resilience* is not merely a protective mechanism but a determinant of strategic advantage. Its absence magnifies adversarial payoff; its presence constrains hostile influence, preserves decision integrity, and enhances *adaptive deterrence*.

The academic debate on *cognitive resilience* emerges from a broader attempt to conceptualise how modern warfare increasingly targets, not only forces, platforms, and infrastructure, but also perception, judgment, attention, trust, and decision cycles. In EU-oriented discussions, *cognitive warfare* is framed as a security-policy challenge produced by digital acceleration, narrative contestation, and the strategic exploitation of societal vulnerabilities (Ariton 2025). Military-oriented analyses similarly emphasise that the "battlefield" expands into the digital gray zone, where adversaries seek decision disruption, behavioural steering, and legitimacy erosion rather than immediate kinetic outcomes (Cheatham et al. 2024). Yet an important limitation in this emerging literature is conceptual "inflation": *cognitive warfare* can become an umbrella label for disinformation, psychological operations, cyber disruption, and influence campaigns. Comparative syntheses warn that without careful boundary-setting, the concept risks losing analytic value and collapsing into older categories under a newer name (Deppe, Fotescu, & Schaal 2024). This is why conceptual work grounded in NATO's exploratory framing is pivotal: it clarifies *cognitive warfare* as a strategic logic oriented toward *cognitive effects*, not merely the circulation of content (Deppe & Schaal 2024). Even when NATO-derived definitions remain exploratory, their value lies in establishing a minimum conceptual discipline: (1) identify the intended cognitive effect, (2) distinguish vectors from outcomes, and (3) connect tactical influence to strategic decision consequences.

From this conceptual baseline, the literature increasingly pivots from "what *cognitive warfare* is" to "what must be protected", giving rise to the notion of *cognitive security*. *Cognitive security* reframes the human mind and other cognitive assets as objects of protection, proposing that hostile influence constitutes a security threat when it measurably degrades cognitive integrity and decision reliability (Ask et al. 2025). This move is theoretically productive because it connects security studies to cognitive science, but it also raises a critical normative question: the protection of cognition should not become a pretext for intrusive governance or ideological control. A more defensible direction is offered by architecture-informed approaches that translate *cognitive security* into design principles: how systems, interfaces, training, and governance can reduce cognitive attack surfaces while preserving democratic constraints (Doherty 2023). The human-factors perspective strengthens this line by arguing that *cognitive security* must be operationalised through attention to workload, bias, trust calibration, and decision-making conditions, some areas where empirical measurement and intervention are plausible (Tossell et al. 2025). Taken together, these works imply that *cognitive resilience* can be treated as a *strategic asset* only if it is linked to measurable *cognitive performance* and *decision integrity*, rather than remaining at the level of metaphor.

A coherent theoretical framework must therefore integrate *cognitive security* with the broader and contested concept of *resilience*. In security studies, *resilience* is not simply a benign capacity; it is also a political and performative discourse that can shift responsibility onto individuals and communities while obscuring the structural origins of risk (Brassett & Vaughan-Williams 2015). This critique is essential for *cognitive resilience* research: "be resilient" can become an implicit demand that soldiers and citizens absorb informational violence and adapt to manipulation rather than

preventing it. To avoid that trap, governance-centered accounts argue for *resilience* as a managed, institutionalised capability, assessed, coordinated, and continuously improved through policy, accountability, and cross-sector design (Linkov & Trump 2019; Heinimann & Hatfield 2017). Complexity-informed models add an important nuance: *resilience* is not stable "hardening", but the capacity to navigate dynamic order/disorder transitions, where a rigid control may fail and adaptive mechanisms matter (Normandin & Therrien 2016). Because the *cognitive warfare* thrives on ambiguity, overload, and uncertainty, these complexity insights are not peripheral, they are directly relevant to how *cognitive resilience* should be conceptualised as an operational capability rather than a generic psychological virtue.

The *strategic asset* claim becomes most convincing where *resilience* is linked to *deterrence* and *strategic competition*. *Resilience* is theorised as *adaptive deterrence*, shaping adversary calculations by reducing the payoff of coercion and influence operations (Laine & Petersson 2025). This reframing is valuable: *cognitive resilience* is not only defensive recovery, but a capability that can deny strategic effects by preserving decision coherence and societal trust under pressure. However, this *deterrence* argument must be anchored in mechanisms rather than slogans. *Organisational resilience* scholarship supports that anchoring by focusing on the cognitive dimension of *resilience* capacity, emphasizing sensemaking, attention control, and interpretive processes that shape how systems adapt (Lengnick-Hall, Beck & Woznyj 2023). At the human performance level, *strategic resilience* is also discussed as an enabling condition for sustained performance in high-stakes environments, suggesting that *cognitive resilience* has implications for training, education, and performance governance (Ziehr & Merkt 2024). The conceptual synthesis here is straightforward: *cognitive resilience* becomes *strategic* when it demonstrably protects the cognitive prerequisites of *deterrence*: credible signaling, coherent decision cycles, and institutional legitimacy.

A decisive contribution of the recent literature is the explicit coupling of the cognitive domain with *cyber governance* and *technological architectures*. Rather than treating cyber and cognition as separate domains, governance-oriented accounts argue that *cognitive resilience* is necessary for cyber governance itself, because security decisions depend on trust, judgment, and the management of information overload (Grobler & Aamir 2024). Technology-architecture approaches go further by proposing integrated governance models for cyber and *cognitive resilience*, which is an important move for operational environments where digital systems, AI-enabled media, and human cognition form a single socio-technical system (Kaleeva, Blagoev & Shalamanov 2025). Conference-based contributions similarly interpret *cyber resilience* as a prerequisite for confronting *cognitive warfare*, but they are strongest when they specify the chain from technical vector to cognitive effect and decision disruption (Radu 2025; Meghraoui & Belkhamza 2025). In parallel, broader security literature on hybrid threats provides the strategic context in which such convergence matters: hybrid environments blend military and nonmilitary means, making it increasingly artificial to separate "technical" from "cognitive" lines of effort (Kaczmarek & Cholewińska 2024). A national-level discussion of AI as a vector of insecurity reinforces the same logic: AI scales persuasion, deception, and targeting, making cognitive vulnerabilities strategically exploitable (Peptan 2025).

The most operationally consequential sub-field concerns *disinformation, psychological operations,* and *cognitive inoculation*. Military-facing work on "information inoculation" argues for preparing warfighters to resist manipulation through preemptive cognitive training, which is an approach aligned with psychological inoculation theory, but requiring careful implementation to avoid indoctrination dynamics (Bebber 2025). Empirical work on *resilience* to disinformation is particularly valuable because it identifies correlates and countermeasures, offering a bridge between concept and measurement (Mider & Żółtowski 2025). Education-based interventions likewise demonstrate that *resilience* can be built through diagnostic and training programs, especially in contexts of war-related disinformation (Molek-Kozakowska 2024). At the operational edge, cyber-enabled psychological and information operations show how influence campaigns are increasingly fused with digital vectors, reinforcing the need for integrated threat models (Mlejňková 2022). A

recurring limitation across this cluster, however, is the tendency to treat *disinformation resilience* as a proxy for *cognitive resilience* overall. A stronger theoretical framework should treat disinformation as one pathway among several, alongside overload, fear induction, identity polarisation, trust erosion, and decision paralysis, and explicitly show how these pathways degrade strategic decision-making.

Recent work on *AI-driven disinformation* further intensifies this imperative. Policy-oriented analyses argue that AI changes the scale, speed, personalisation, and credibility of manipulative content, requiring *democratic resilience* measures that span regulation, platform governance, and societal preparedness (Romanishyn, Malytska & Goncharuk 2025). Yet, the strategic relevance of this literature depends on linking policy prescriptions to cognitive mechanisms: how deepfakes, synthetic persuasion, and coordinated inauthentic behaviour affect trust calibration, epistemic vigilance, and institutional legitimacy. Complementing these discussions, broader treatments of *psychological warfare* in the digital age provide descriptive taxonomies of strategies and impacts, though they vary in rigor and should be used selectively where they add conceptual clarity rather than repetition (Nawaz 2025).

The military specificity of *cognitive resilience* is reinforced where studies address *personnel factors* and *human-AI teaming*. Assessments focused on military personnel identify critical factors shaping *cognitive resilience*, offering a rare step toward operationalisation in defence contexts (Kosárová, Bízík & Potočňák 2024). In future force design, the challenge is not only to "train resilient minds", but to design socio-technical teams whose interfaces and adaptive systems protect decision quality under adversarial conditions. Neuroadaptive and human-AI teaming perspectives explicitly connect *cognitive resilience* to operational integrity and decision superiority, implying that *resilience* must be engineered into the system rather than treated as an individual trait (Picchi 2025). Service and staff papers can add context for doctrine and professional military education, but their theoretical value depends on whether they contribute unique operational logic rather than reiterating general claims (Delmonte 2024). Military-oriented analyses demonstrate that *cognitive warfare* directly targets command-and-control effectiveness by exploiting cognitive biases, information overload, and digitally mediated manipulation, thereby degrading sensemaking and decision-action cycles before kinetic engagement occurs. Drawing on the Canadian Armed Forces context, Delmonte shows that systematic training in media and information literacy and critical thinking constitutes a core mechanism for strengthening *cognitive resilience*, positioning it as a prerequisite for *cognitive security* and decision integrity in multi-domain operations (Delmonte 2024).

Finally, a strategic framework must position *cognitive resilience* within *whole-of-society and national resilience architectures*. European security discussions emphasise *cognitive resilience* as part of broader *resilience* agendas and geopolitical contestation, including region-specific insights that show how societal context shapes cognitive vulnerabilities and defences (Hansen 2017; Senčar 2021). Policy and best-practice reports emphasise institutional coordination, public communication, and cross-sector measures for countering hybrid threats, some elements that directly support the claim that *cognitive resilience* has strategic effects beyond the military (Wigell, Mikkola & Juntunen 2021; Teperik et al. 2018). Contemporary Ukrainian recommendations provide a particularly relevant illustration of how *cognitive resilience* can be embedded into national security planning, including links to defence-economic dimensions and state capacity (Semenenko et al. 2025). Youth-oriented *resilience* initiatives in the Baltics highlight intergenerational and societal dimensions, though their integration into a warfare-focused argument must be carefully justified to avoid drifting into general social policy (Teperik, Denisa-Liepniece & Bankauskaitė 2025). *Socioeconomic resilience* comparisons can also supply contextual variables, such as trust, cohesion, and sustainability conditions, that shape a society's baseline vulnerability to cognitive operations (Šimelytė, Vveinhardt & Deikus 2025). Where regionally specific analyses frame *cognitive resilience* against *cognitive warfare* targeting a particular state, the contribution is strongest when it offers transferable components and enhancement strategies rather than purely national narratives (Torabi & Ahmadi 2025). Works that attempt to synthesise "*societal resilience* through education vs. war" can be conceptually useful, but while societal, state, and *military resilience* are conceptually developed in existing literature, the *cognitive resilience* remains under-theorised and

insufficiently operationalised, despite being implicitly acknowledged as a critical dimension of contemporary security (Lesenciuc, Nagy & Lesenciuc 2022).

Overall, the reviewed sources justify a consolidated theoretical claim: *cognitive resilience* functions as a *strategic asset* when it is treated as a governed, designed, and measurable capability that protects decision integrity across military and societal levels. The strongest trajectory in the literature moves from definitional clarity (Cheatham et al. 2024; Deppe & Schaal 2024.), to *cognitive security* architecture (Ask et al. 2025; Doherty 2023), to *resilience governance* and *deterrence* (Brassett & Vaughan-Williams 2015; Laine & Petersson 2025), and finally to operationalisation through human factors, personnel assessment, and socio-technical design (Tossell et al. 2025; Kosárová, Bízík & Potočňák 2024; Picchi 2025). The main constructive gap remains methodological: the field still needs more explicit indicators and evaluation designs that can demonstrate how *cognitive resilience* reduces adversary payoff, stabilises decision cycles, and strengthens *deterrence* under conditions of hybrid and AI-enabled influence.

3. Security Implications

The conceptualisation of *cognitive resilience* as a *strategic asset* carries significant implications for contemporary security policy, military doctrine, and institutional governance. As recent literature on *cognitive warfare* and *cognitive security* demonstrates, modern adversaries increasingly target cognitive processes rather than exclusively physical assets, seeking to degrade perception, judgment, trust, and decision-making coherence (Cheatham et al. 2024; Deppe & Schaal 2024). In this context, security is conceptualised as a multidimensional construct that has long transcended purely military and state-centric interpretations, incorporating the societal and human dimensions, as reflected in established approaches such as the Copenhagen School and the human security paradigm. From this perspective, the cognitive and perceptual factors extend beyond explanatory variables, positioning the integrity of cognition itself as an emerging security concern (Ask et al. 2025).

At the strategic level, *cognitive resilience* reshapes prevailing understandings of *deterrence*. Classical *deterrence* models focus on material capabilities and credible threats of retaliation, yet hybrid and *cognitive warfare* strategies aim to circumvent these mechanisms by undermining decision cycles, institutional confidence, and societal cohesion (Ariton 2025; Kaczmarek & Cholewińska 2024). As argued in recent *resilience* scholarship, *resilience* functions as a form of *adaptive deterrence*, reducing the strategic utility of coercive influence by denying adversaries the cognitive effects they seek to achieve (Laine & Petersson 2025). *Cognitive resilience*, understood in this sense, signals that attempts to manipulate perceptions or destabilise decision-making will fail to produce strategic gains, thereby constraining adversarial behaviour.

At the *operational and organisational level*, the findings imply a necessary shift away from viewing *resilience* as an individual psychological trait toward treating it as an *institutionally governed capability*. Research on *cognitive security* and human factors underscores that decision quality depends not only on individual robustness but on organisational design, workload distribution, information management, and shared situational awareness (Doherty 2023; Tossell et al. 2025). Governance-oriented approaches to *resilience* further emphasise that institutions must embed procedures for anticipating, absorbing, and adapting to cognitive disruption as a routine element of security practice (Linkov & Trump 2019; Heinimann & Hatfield 2017). Without such institutionalisation, even cognitively capable individuals remain vulnerable within poorly designed systems.

The study also highlights the security relevance of *passive cognitive stressors*, which are often underestimated in strategic planning. Prolonged operational tempo, cognitive fatigue, emotional strain, and sustained exposure to contested information environments gradually erode cognitive performance and increase susceptibility to hostile influence (Vrijkotte et al. 2016; Flood & Keegan 2022). Empirical and conceptual work indicates that such passive stressors significantly amplify the effectiveness of active cognitive operations, including disinformation and psychological pressure (Mider & Żółtowski 2025;

Mlejňková 2022). Consequently, security policies that focus exclusively on countering external adversaries while neglecting internal cognitive conditions risk unintentionally enhancing adversarial impact.

From a *whole-of-society security perspective*, *cognitive resilience* extends beyond military and governmental institutions to encompass societal trust, communication ecosystems, and civil-military relations. Hybrid threat research consistently shows that *cognitive warfare* frequently targets social cohesion and institutional legitimacy rather than immediate physical damage (Wigell, Mikkola & Juntunen 2021). Case-based analyses from Europe and Ukraine further demonstrate that societies with higher levels of *cognitive preparedness*, manifested in credible public communication, critical information literacy, and institutional coordination, are better positioned to withstand sustained influence campaigns (Hansen 2017; Teperik et al. 2018; Semenenko et al. 2025). *Cognitive resilience* thus becomes a prerequisite for maintaining national security under conditions of persistent informational pressure.

The convergence of *cognitive, cyber, and AI-enabled threats* introduces additional governance challenges. Recent studies emphasise that AI-driven disinformation and automated influence operations accelerate the scale, personalisation, and credibility of cognitive attacks, blurring traditional boundaries between cyber security and psychological operations (Romanishyn, Malytska & Goncharuk 2025; Meghraoui & Belkhamza 2025). Governance models that integrate *cyber* and *cognitive resilience* highlight the necessity of combining technological safeguards with organisational and cognitive defences, rather than treating these domains in isolation (Grobler & Aamir 2024; Kaleeva, Blagoev & Shalamanov 2025).

Finally, the study implies a need to rethink security preparedness and evaluation metrics. Conventional indicators, such as force structure, response time, or technological inventories, fail to capture vulnerabilities in the cognitive domain. Emerging research on human performance and *military personnel resilience* suggests that cognitive robustness, decision integrity, and adaptive capacity under informational stress should be incorporated into security assessments (Kosárová, Bízík & Potočňák 2024; Ziehr & Merkt 2024). Although the present study remains conceptual, it provides the theoretical basis for developing such indicators in future empirical research.

In sum, the security implications of *cognitive resilience* are both structural and strategic. Treating *cognitive resilience* as a *strategic asset* requires a shift from reactive countermeasures toward proactive governance of cognitive capacity, from individual coping toward institutional design, and from narrow threat mitigation toward sustained decision integrity (Brassett & Vaughan-Williams 2015). In contemporary warfare environments, where influence, ambiguity, and perception increasingly determine outcomes, *cognitive resilience* emerges as a decisive enabler of security, stability, and strategic autonomy.

Conclusions

This conceptual and theoretical analysis builds on and systematises existing strands of the literature to articulate an integrated analytical framework for understanding cognitive resilience as a strategic asset in contemporary warfare. First, the reviewed studies consistently indicate that cognitive resilience acquires strategic relevance primarily when it is conceptualised, governed, and operationalised at the organisational and institutional level, rather than approached solely as an individual psychological capacity. Second, the literature converges on the view that passive cognitive stressors, such as fatigue, information overload, and prolonged uncertainty, constitute enabling conditions that amplify the impact of active cognitive warfare stressors, thereby increasing the vulnerability to manipulation and decision degradation.

This study has argued that *cognitive resilience* must be understood as a security-relevant, governable capability that protects the cognitive foundations of decision-making, institutional legitimacy, and *strategic coherence* in contemporary warfare. By integrating behavioural science insights with security studies, governance theory, and *cognitive warfare* literature, the analysis

demonstrates that *resilience* is not merely a reactive coping mechanism but a proactive strategic resource that constrains adversarial influence and supports *adaptive deterrence*. *Cognitive resilience* becomes strategically meaningful when it preserves decision integrity under pressure, stabilizes sensemaking processes, and reduces the strategic payoff of cognitive attacks.

A central contribution of this research lies in its systematic distinction between active and passive cognitive stressors, and in demonstrating their interactive effects on cognitive vulnerability. While *cognitive warfare* literature often focuses on intentional influence operations, this study shows that unmanaged internal conditions, such as organisational overload, sustained stress, and cognitive depletion, can be equally decisive in shaping security outcomes. Consequently, *cognitive resilience* cannot be achieved through counter-disinformation measures alone but requires institutional design, workload governance, and sustained cognitive capacity management.

The study further advances the field by linking *cognitive resilience* to *cognitive security* and *adaptive deterrence*, positioning it within broader strategic competition rather than treating it as a peripheral psychological concern. In doing so, it reframes *resilience* from a discourse of endurance and responsibilisation into one of strategic governance and institutional responsibility. This reframing is particularly relevant in hybrid and AI-enabled conflict environments, where adversaries increasingly seek to disrupt decision cycles and societal trust without crossing traditional thresholds of armed conflict.

From a security policy perspective, the analysis underscores the necessity of integrating *cognitive resilience* into military doctrine, organisational governance, and whole-of-society security frameworks. Protecting cognitive assets, such as attention, judgment, trust calibration, and decision coherence, emerges as a prerequisite for effective deterrence, crisis management, and strategic autonomy. The study therefore provides a theoretical foundation for future empirical research, capability development, and policy design aimed at operationalising *cognitive resilience* across military, governmental, and societal levels.

BIBLIOGRAPHY:

Ariton, Lorina. 2025. Cognitive Warfare In The Digital Age: Implications For Eu Security Policy. In: International Conference Knowledge-Based Organization, pp. 1-9. doi: 10.2478/kbo-2025-0001.

Ask, T. F.; Sütterlin, S.; Müller, M.; Lugo, R. G.; Saari, D.; Grahn, H.; Canhame, M.; Hermansen, D. and Knox, B.J. 2025. Cognitive Security: The study and practice of protecting the human mind and other Cognitive Assets from cognitive threats. PsyArXiv preprint. doi: 10.31234/osf.io/2ftqc_v1.

Bebber, R. 2025. Information inoculation: preparing US warfighters for cognitive war. Hudson Institute.

Bierecki, Dominik; Gaie, C.; Karpiuk, M. and Langlois-Berthelot, J. 2025. Creating Resilient Artificial Intelligence Systems. A Responsible Approach to Cybersecurity Risks. Prawo i Więź, nr. 5 (58) październik, 131-149.

Brassett, J. and Vaughan-Williams, N. 2015. Security and the performative politics of resilience: Critical infrastructure protection and humanitarian emergency preparedness. Security Dialogue, 2015, 46(1), 32–50. doi:10.1177/0967010614555943.

Cheatham, Michael J.; Geyer, Angelique M.; Nohle, Priscella A. and Vazquez, Jonathan E. 2024. Cognitive Warfare: The Fight for Gray Matter in the Digital Gray Zone. Joint Force Quarterly 114 (3rd Quarter 2024), 83-91, https://digitalcommons.ndu.edu/joint-force-quarterly/vol114/iss2/15 (21.12.2025)

Claverie, B. and Du Cluzel, F. 2022. "Cognitive warfare": The advent of the concept of "cognitics" in the field of warfare. Cognitive Warfare: the future of cognitive dominance, 2-1, 1-7, 2022, 978-92-837-2392-9. ffhal-03635889f.

Delmonte, Major Alexandra L. 2024. JCSP 51 - PCEMI n° 51 Service Paper Étude militaire. 2024-2025.

Deppe, Christoph; Fotescu, Alexandru and Schaal, Gary 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, Hamburg Germany: NATO S&T.

Deppe, Christoph and Schaal, Gary S. 2024. Cognitive warfare: a conceptual analysis of the NATO ACT cognitive warfare exploratory concept. Frontiers in Big Data, 2024, 7: 1452129. https://doi.org/10.3389/fdata.2024.1452129

Doherty, G. 2023. Cognitive Security: An Architecture Informed Approach from Cognitive Science. In: Schmorrow, D.D., Fidopiastis, C.M. (eds) Augmented Cognition. HCII 2023. Lecture Notes in Computer Science, vol 14019. Springer, Cham. https://doi.org/10.1007/978-3-031-35017-7_25

Elman, J. A., Vogel, J. W., Bocancea, D. I., Ossenkoppele, R., van Loenhoud, A. C.; Tu, X. M. and Kremen, William S. 2022. Issues and recommendations for the residual approach to quantifying cognitive resilience and reserve. Alzheimer's research & therapy, 14(1), 102. doi:10.1186/s13195-022-01049-w.

Flood, A. and Keegan, R. J. 2022. Cognitive resilience to psychological stress in military personnel. Frontiers in psychology, 13, 809003. doi: 10.3389/fpsyg.2022.809003.

Grobler, Marthie and Aamir, Tooba. 2024. Building cognitive resilience for enhanced cyber governance. In: Psybersecurity. CRC Press, pp. 52-72. http://hdl.handle.net/102.100.100/637002?index=1

Hansen, Flemming Splidsboel. 2017. Cognitive Resilience in Central Asia. In: N. Popescu, & F. Gaub (eds.), After the EU Global Strategy – Building Resilience European Union Institute for Security Studies, 2017, pp. 73-75. http://www.iss.europa.eu/publications/detail/article/after-the-eu-global-strategy-building-resilience/ (13.01.2026)

Heinimann, Hans R. and Hatfield, Kirk. 2017. Infrastructure resilience assessment, management and governance–state and perspectives. In: Linkov, I., Palma-Oliveira, J. (eds) Resilience and Risk. NATO Science for Peace and Security Series C: Environmental Security. Springer, Dordrecht, pp. 147-187. https://doi.org/10.1007/978-94-024-1123-2_5

Kaleeva, Tiana; Blagoev, Ivan and Shalamanov, Velizar. 2025. Governance Model and Technology Architecture in Developing Cyber and Cognitive Resilience. In: Digital Technologies for Enhancing Resilience. IOS Press, pp. 227-243.

Kaczmarek, Krzysztof and Cholewińska, Dagmara. 2024. Security and Hybrid Threats. Przegląd Nauk o Obronności, (20):91-100. https://doi.org/10.37055/pno/208458

Kosárová, Dominika; Bízik, Vladimír and Potočňák, Adam. 2024. Cognitive Resilience: Assessing Critical Factors in Military Personnel. Univerzita Obrany. Ustav Strategickych Studii. Obrana a Strategie, 2: 133-156.

Laine, Jussi P. and Petersson, Bo. 2025 Resilience as Adaptive Deterrence in an Era of Strategic Uncertainty. In: Resilience as Deterrence: Towards a Comprehensive Security Panorama, Jussi P. Laine and Bo Petersson (eds.), NATO science for peace and security series. Sub-series E, Human and societal dynamics, ISSN 1874-6276, E-ISSN 1879-8268; 159, IOS Press, pp. 1-19.

Lengnick-Hall, Cynthia; Beck, Tammy and Woznyj, Haley Myers. 2023. What are you Thinking?: Understanding the Cognitive Dimension of Resilience Capacity. In: Resilience in Modern Day Organizations. Routledge, pp. 7-25.

Lesenciuc, Adrian; Nagy, Daniela and Lesenciuc, Simona. 2022. Societal Resilience. Between Resilinece Through Education and Resilience Through War. Redefining Community in Intercultural Context, 10(1), 25-31.

Linkov, I. and Trump, B.D. Resilience and Governance. 2019. In: The Science and Practice of Resilience. Risk, Systems and Decisions. Springer, Cham. https://doi.org/10.1007/978-3-030-04565-4_5

Meghraoui, Loukmane and Belkhamza, Zakariya. 2025. Cognitive Warfare and Cybersecurity: Strategic Implications for Global Security. In: Proceedings of the 19th International Conference on Cyber Warfare and Security 2025, editors Stephanie J. Blackmonand and Saltuk Karahan, pp. 257-264.

Mider, Daniel and Żółtowski, Marcin. 2025. Correlates of Poles' Resilience to Disinformation – Opinions and Countermeasures. Democracy and Security, 1-30. https://doi.org/10.1080/17419166.2025.2525756

Mlejnková, Petra. 2022. Issues of resilience to cyber-enabled psychological and information operations. Vojenské rozhledy, 31.1: 38-50.

Molek-Kozakowska, Katarzyna. 2024. Enhancing Resilience Against War-Related Disinformation: Insights from Diagnostic Studies and Interventions at Polish Schools. Revista Transilvania, 9, 65-76. https://doi.org/10.51391/trva.2024.09.07.

Nawaz, Faisal. 2025. Psychological Warfare in the Digital Age: Strategies, Impacts, and Countermeasures. Journal of Future Building, 2.1: 21-30.

Normandin, Julie-Maude and Therrien, Marie-Christine. 2016. Resilience Factors Reconciled with Complexity: The Dynamics of Order and Disorder. Journal of Contingencies and Crisis Management, 2016, 24(2), 107-118. doi:10.1111/1468-5973.12107.

Parsons, S., Kruijt, A. W., and Fox, E. 2016. A cognitive model of psychological resilience. Journal of Experimental Psychopathology, 7(3), 296-310.

Peptan, Cătălin. 2025. Romania Facing New Vectors of Insecurity: Hybrid Warfare and Artificial Intelligence, Research and Science Today, 2(30), 87-106, doi: 10.38173/RST.2025.30.2.8:87-106.

Picchi, Andrea. 2025. Designing for Cognitive Resilience in Human-AI Teams: A Neuroadaptive Approach to Operational Integrity and Decision Superiority. https://www.researchgate.net/publication/392933806_Designing_for_Cognitive_Resilience_in_Human-AI_Teams_A_Neuroadaptive_Approach_to_Operational_Integrity_and_Decision_Superiority (27.12.2025)

Radu, Raluca.2025. Building Cyber Resilience to Face the Challenges of Cognitive Warfare. In: European Conference on Cyber Warfare and Security. Academic Conferences International Limited, pp. 803-810.

Romanishyn, Alexander; Malytska, Olena and Goncharuk, Vitaliy. 2025. AI-driven disinformation: policy recommendations for democratic resilience. Frontiers in Artificial Intelligence, 8: 1569115. doi:10.3389/frai.2025.1569115.

Semenenko, Oleh; Kin, Oleksandr; Semenenko, Liliia; Remez, Volodymyr; Serhii Mytchenko and Rybak, Dmytro. 2025. Ключові кроки України в системі воєнної та національної безпеки щодо підвищення когнітивної стійкості (2025-2028 рр.): рекомендації у когнітивній та воєнно-економічній сфері/ Key Steps of Ukraine in the Military and National Security System to Increase Cognitive Resilience (2025-2028): Recommendations in the Cognitive and Military-Economic Spheres. Social Development and Security, 15.4: 36-49. https://doi.org/10.33445/sds.2025.15.4.4

Senčar, Igor. 2021. Kognitivni Vidiki Evropskih Varnostnih In Obrambnih Izzivov/ The Cognitive Aspects of Europe's Security and Defence Challenges. Contemporary Military Challenges/ Sodobni Vojaški Izzivi, 23.3. doi:10.33179/BSV.99.SVI.11.CMC.23.3.1.

Šimelytė, Agnė; Vveinhardt, Jolita; Deikus, Mykolas. 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. ISSN 2345-0355 https://doi.org/10.15544/mts.2025.15.

Staal, M. A., Bolton, A., Yaroush, R., and Bourne, L. 2008. Cognitive performance and resilience to stress. In: Biobehavioral Resilience to Stress. eds. B. J. Lukey and V. Tepe (Boca Raton, FL: CRC Press), 259-299.

Teperik, Dmitri; Jermalavičius, Tomas; Senkiv, Grigori; Dubov, Dmytro; Onyshchuk, Yevhen; Samus, Mykhailo, and Pokalchuk, Oleh. 2018. A Route to National Resilience. Building. Whole-of-Society Security in Ukraine. URL: https://uploads.icds. ee/ICDS_Report_A_Route_oilience-Building. (12.01.2026)

Torabi, Hassan and Ahmadi, Fatemeh. 2025. Cognitive Resilience against Cognitive Warfare Targeting Iran: Components, Analysis, and Enhancement Strategies. Cognitive research of political studies, 2.1: e219219. (09.01.2026)

Teperik, Dmitri; Denisa-Liepniece, Solvita and Bankauskaitė, Dalia. 2025. GLUED: Linking Resilience and Youth Futures in the Baltics. Report. Tallinn Riga Vilnius. 10.13140/RG.2.2.12470.77125, ISBN 978-9908-9709-1-2.

Tossell, C. C.; Spencer, C. A.; Endsley, M. R.; Canham, M.; Steckman, L.; Hayman, A. and Hirshfield, L. 2025. Charting New Frontiers in Cognitive Security: A Human Factors Call to Action. Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 0(0). https://doi.org/10.1177/10711813251369366

Vrijkotte, S., Roelands, B., Meeusen, R., and Pattyn, N. 2016. Sustained military operations and cognitive performance. Aerospace medicine and human performance, 87(8), 718-727.

Wigell, Mikael; Mikkola, Harri and Juntunen, Tapio. 2021. Best Practices in the whole-of-society approach in countering hybrid threats. European Parliament Coordinator: Policy Department for External Relations Directorate General for External Policies of the Union. doi:10.2861/379.

Ziehr, S. and Merkt, P.H. 2024. Strategic resilience in human performance in the context of science and education - perspective. Front. Psychiatry, 15:1410296. doi: 10.3389/fpsyt.2024.1410296.