COGNITIVE RESILIENCE AS A NEW DIMENSION OF EUROPEAN UNION SECURITY: CONCEPTUAL DELIMITATIONS AND EPISTEMOLOGICAL FOUNDATIONS

Ruslana GROSU, Cătălin-Victor POPESCU

Armed Forces Military Academy „Alexandru cel Bun", Chisinau, Republic of Moldova,
(ruslana.grosu@gmail.com, popescuvictor546@gmail.com)

DOI: 10.19062/2247-3173.2026.27.9

Abstract: *The paper advances the central argument that cognitive resilience has emerged as a distinct analytical and operational category within contemporary European Union security studies. While related to psychological, societal, and informational resilience, cognitive resilience is conceptualised here as a multidimensional capacity aimed at preserving the integrity, adaptability, and coherence of cognitive processes under conditions of manipulation, disinformation, and epistemic destabilisation.*

Methodologically, the study employs a qualitative, theory-building research design, combining conceptual analysis, systematic review of academic literature and EU strategic documents, and theoretical meta-synthesis across security studies, cognitive warfare doctrine, and cognitive psychology. This interdisciplinary approach enables the clarification of conceptual boundaries and the integration of diverse theoretical perspectives into a coherent analytical framework.

The findings demonstrate that cognitive resilience constitutes a necessary extension of the resilience paradigm, addressing a critical gap in both academic literature and EU policy frameworks. Existing approaches remain predominantly focused on regulating information flows and mitigating external threats, while insufficiently addressing the internal cognitive mechanisms that enable manipulation to be effective. In response, the paper proposes an operational definition of cognitive resilience and identifies its core dimensions, cognitive filtering capacity, interpretative coherence, adaptive flexibility, and epistemic trust, thus enabling future empirical measurement and comparative research.

The study concludes that the integration of cognitive resilience fundamentally expands the security paradigm, repositioning cognition as a central strategic domain and cognitive autonomy as a key determinant of democratic stability. As such, cognitive resilience emerges not merely as a complementary concept, but as a strategic capability essential for the EU's capacity to withstand and adapt to the challenges of contemporary cognitive warfare.

Keywords*: cognitive resilience, cognitive security, European Union security, hybrid threats, disinformation, cognitive warfare, security paradigm transformation.*

1. INTRODUCTION

The European Union's security environment has undergone a profound transformation over the past decade, shaped by the emergence of hybrid threats, the strategic use of disinformation, and the increasing operational relevance of cognitive warfare. These dynamics fundamentally challenge traditional security paradigms, which have historically prioritised territorial defence, military capabilities, and institutional stability as primary referents of security.

In contrast, the contemporary security environment increasingly targets the cognitive domain, influencing perception, belief formation, identity construction, and decision-making processes at both individual and collective levels. In this sense, security can no longer be conceptualised exclusively in material or institutional terms, but must be redefined to include the protection and resilience of cognitive processes themselves.

Recent conceptual and empirical studies highlight that cognitive warfare targets human cognition by influencing and modifying decision-making processes [1, p. 1]. Within the European context, disinformation campaigns have been widely documented, including during the COVID-19 crisis, where state actors such as China engaged in coordinated influence operations [1, p. 3]. These dynamics reveal not only the vulnerability of the EU's information environment but also the erosion of public trust and the growing complexity of internal and external disinformation challenges, which together constrain the Union's capacity to respond coherently [2, pp. 571-573]. Consequently, the strategic environment has evolved toward a configuration in which cognition itself becomes a contested domain, and the capacity to resist manipulation and maintain interpretative coherence emerges as a critical security asset.

Against this backdrop, this study advances the argument that *cognitive resilience* should be conceptualised as a distinct analytical and operational category within European Union security studies, rather than being subsumed under broader constructs such as societal, psychological, or informational resilience. While these related concepts capture important dimensions of systemic adaptability and robustness, they remain insufficient for addressing the specific mechanisms through which cognition is targeted, distorted, and reconfigured in the context of hybrid threats and strategic communication warfare. *Cognitive resilience*, therefore, requires a more precise conceptual delimitation, one that recognizes its unique focus on the integrity, adaptability, and protection of cognitive processes.

To address this conceptual gap, conceptual analysis is employed to clarify the definitional boundaries of *cognitive resilience* and to distinguish it from adjacent constructs, thereby reducing terminological ambiguity and strengthening analytical precision. This is complemented by a systematic review of the relevant literature, aimed at identifying and synthesizing key contributions from security studies, cognitive warfare theory, cognitive psychology, and European Union policy research. Through this process, the study maps the existing body of knowledge, highlighting both convergences and inconsistencies across disciplinary perspectives. Finally, a theoretical meta-synthesis is undertaken in order to integrate these diverse insights into a coherent analytical framework, enabling the formulation of higher-order theoretical propositions regarding the role and function of *cognitive resilience* within contemporary security paradigms.

The selection of sources follows a structured logic grounded in relevance, quality, and interdisciplinarity. Priority is accorded to works that directly engage with the conceptualisation of cognitive warfare and cognitive security, as well as those that address resilience as a strategic construct within the evolving European security architecture [1; 3]. At the same time, particular attention is given to studies that examine disinformation, hybrid threats, and policy responses within the European Union, ensuring that the analysis remains anchored in concrete strategic realities [2; 4; 5]. Given the inherently cross-cutting nature of *cognitive resilience*, the research further integrates contributions from adjacent domains, including cognitive diplomacy, digital warfare, and artificial intelligence-driven disinformation, thereby reflecting the multidimensional character of the phenomenon under investigation [6; 7; 8]. Only peer-reviewed publications, academic conference proceedings, and high-quality policy reports are included, ensuring both scientific rigour and analytical credibility.

By combining these methodological approaches, the study seeks to advance the theoretical consolidation of *cognitive resilience* and to reposition it within the broader field of European Union security studies. Its contribution is threefold: first, it clarifies the epistemological status of *cognitive resilience* as an emerging concept; second, it establishes its analytical autonomy in relation to other resilience frameworks; and third, it proposes a conceptual foundation capable of supporting future operationalisation and empirical investigation. In doing so, the study responds to an increasingly urgent need to reconceptualize security in a manner that adequately reflects the cognitive dimensions of contemporary conflict and strategic competition.

2. THEORETICAL FOUNDATIONS OF COGNITIVE RESILIENCE

The concept of resilience has undergone a significant epistemological transformation within security studies, evolving from a predominantly technical notion associated with infrastructure protection and risk management toward a complex, multi-level analytical framework encompassing societal, institutional, and cognitive dimensions. In its early formulations, resilience was primarily understood in engineering and infrastructure contexts as the capacity of systems to resist disruption, maintain critical functions, and recover after adverse events, with a strong emphasis on robustness and post-event recovery processes [9, pp. 147-149]. However, the increasing complexity of interconnected socio-technical systems and the evolving nature of contemporary security challenges have driven a conceptual expansion of resilience beyond material infrastructures toward societal and informational domains [10, p. 24; 5, p. 12].

The conceptual differentiation between resilience in its general sense, psychological resilience, societal resilience, informational resilience, and, in particular, *cognitive resilience* constitutes a fundamental prerequisite for theoretical rigour in advanced security studies research. In the context of deeper research, where conceptual precision and epistemological clarity are essential evaluative criteria, the uncritical or interchangeable use of these constructs frequently leads to analytical ambiguity and weakens argumentative coherence. It is therefore necessary to reconstruct these notions within an integrated analytical framework, drawing on the literature from security studies, cognitive psychology, and European Union policy.

In its broadest sense, resilience functions as an umbrella concept, denoting the capacity of a system to absorb shocks, adapt, and maintain or regain functionality under conditions of disruption. Subsequently, the concept has been progressively extended within security studies to encompass broader societal and institutional dimensions, reflecting the increasing complexity of contemporary threat environments. In a foundational contribution, C.S. Holling defined resilience as a measure of the persistence of ecological systems, referring to their ability to absorb disturbances while maintaining the integrity of relationships between state variables, thereby distinguishing it from stability, understood as the capacity to return to equilibrium [11, p. 14]. This conceptualisation has profoundly influenced subsequent theoretical developments across multiple disciplines. Nevertheless, despite its analytical versatility, resilience has been criticised for its conceptual breadth, often functioning as a “catch-all” notion lacking clearly defined boundaries and operational precision [12, p. 3].

A more narrowly defined construct is that of psychological resilience, which refers to the individual’s capacity to cope with stress, trauma, and adversity while maintaining psychological stability and functional equilibrium. Foundational contributions by M. Rutter conceptualise resilience not as a fixed trait, but as a dynamic process shaped by the interaction between risk and protective factors operating over time [13, p. 316].

Similarly, A.S. Masten defines resilience as a class of phenomena characterised by positive adaptation in the context of significant adversity, famously describing it as "ordinary magic", thereby emphasising the normative and widespread nature of adaptive capacities [14, p. 227]. G.A. Bonanno further conceptualises resilience as the ability to maintain relatively stable, healthy levels of psychological functioning following potentially traumatic events, distinguishing it from recovery processes [15, p. 20]. This form of resilience operates predominantly at the individual level and is primarily concerned with coping mechanisms, emotional regulation, and trajectories of adaptation following adversity, being situated within the domains of clinical psychology, developmental psychology, and mental health research. However, from the perspective of security studies, psychological resilience presents important limitations: it does not sufficiently account for the mechanisms through which individuals process information, nor does it address vulnerability to cognitive manipulation, disinformation, or strategic influence operations.

At the macro level, societal resilience has become a central concept within European security policy. The European Union Global Strategy (2016) emphasises the resilience of states and societies, implicitly framing it as the capacity to withstand and adapt to internal and external crises [10, p. 24]. This conceptualisation aligns with earlier sociological approaches, such as those proposed by W.N. Adger, who defines social resilience as the ability of communities to cope with external stresses and disturbances [16, p. 347], and F.H. Norris, S.P. Stevens, B. Pfefferbaum, K.F. Wyche, R.L. Pfefferbaum, who conceptualise it as a set of adaptive capacities, such as economic development, social capital, information and communication, and community competence, that enable collective adaptation and recovery [17, p.130].

Within the EU framework, societal resilience encompasses dimensions such as institutional robustness, governance capacity, social cohesion, and economic stability, and is closely linked to the management of hybrid and cyber threats. Nevertheless, this conceptualisation remains predominantly structural and institutional in orientation and does not sufficiently explain the cognitive mechanisms through which vulnerabilities are generated, internalised, and exploited.

While the European Union's emphasis on societal resilience represents a significant step toward addressing the multidimensional nature of contemporary security challenges, its predominantly structural and institutional orientation leaves a critical analytical gap. Specifically, it does not sufficiently account for the cognitive processes through which individuals and societies interpret information, construct meaning, and ultimately make decisions in environments characterised by uncertainty, manipulation, and strategic influence.

In this context, the increasing prevalence of disinformation, hybrid threats, and cognitive warfare highlights the limitations of existing resilience frameworks, which tend to prioritise systemic robustness over epistemic integrity. As contemporary conflicts increasingly target perception, belief formation, and decision-making processes, the locus of vulnerability shifts from external systems to internal cognitive mechanisms.

Addressing this gap requires a reconceptualisation of resilience that explicitly incorporates the cognitive dimension of security. Accordingly, this study advances the concept of *cognitive resilience* as a distinct analytical and operational category, defined as the capacity of individuals and societies to maintain the integrity, coherence, and autonomy of cognitive processes under conditions of informational pressure and strategic manipulation.

A related but distinct concept is that of informational resilience, which primarily focuses on the robustness of information systems and the capacity to manage, regulate, and secure information flows.

Its analytical focus is situated at the level of digital platforms, media ecosystems, and technological infrastructures that mediate the production and dissemination of information. While this perspective is essential for understanding the structural architecture of contemporary information environments, it tends to conceptualise information as an object of circulation rather than as a process of interpretation. As such, it remains insufficiently equipped to capture the cognitive mechanisms through which information is perceived, filtered, and transformed into meaning.

Within this fragmented conceptual landscape, *cognitive resilience* emerges as a distinct and necessary analytical category. Unlike other forms of resilience, which are primarily oriented toward systems, emotional adaptation, or infrastructural robustness, *cognitive resilience* is centred on the processes through which reality itself is perceived, interpreted, and understood. It can be defined as the multidimensional capacity of individuals, groups, and institutions to preserve the integrity, coherence, and autonomy of cognitive processes, such as perception, interpretation, and judgment, under conditions of informational manipulation and strategic influence. Importantly, *cognitive resilience* operates across multiple levels of analysis, encompassing individual cognition, societal dynamics, and institutional frameworks, with cognition, namely the processing and construction of meaning, constituting its core domain.

This distinction becomes particularly salient when comparing the protective functions associated with different forms of resilience. General resilience is primarily concerned with safeguarding system functionality; psychological resilience with maintaining individual emotional stability; societal resilience with preserving the cohesion and stability of social structures; and informational resilience with securing the integrity of information flows. By contrast, *cognitive resilience* targets the preservation of meaning-making processes, thereby introducing an explicitly epistemic dimension into security analysis. This shift is critical, as it reorients the focus of resilience from external systems to internal processes of interpretation, placing interpretative coherence and cognitive autonomy at the centre of security concerns.

The strategic significance of this reconceptualisation is confirmed by NATO doctrinal literature, which identifies cognitive warfare as extending beyond information manipulation to shape the very cognitive processes through which individuals construct meaning and make decisions [18, p. 3]. This is further elaborated in NATO's strategic and scientific frameworks, which emphasise that cognitive warfare aims to alter and shape the way humans think, react, and make decisions, exploiting vulnerabilities in perception, sensemaking, and judgement across individual and collective levels [19, pp. ES-1-ES-2]. The cognitive domain thus emerges not merely as an extension of the informational environment, but as a distinct operational space in which meaning-making processes themselves become the primary target of strategic action.

From this perspective, cognitive warfare represents a paradigmatic shift from informational dominance to cognitive dominance, where the central objective is to influence or disrupt the construction of reality at the level of the human mind. As B. Claverie argues, this form of conflict constitutes an "invisible war" that directly targets thought, rationality, and the conditions of cognition itself, aiming to alter or degrade the normal functioning of cognitive processes [20, pp. 91-92]. This is further reinforced by approaches that conceptualise cognitive warfare as the "war of the brains", focusing on the alteration of cognitive capacities and the manipulation of how individuals think and act [21, pp. 67-68].

Consequently, effective responses to such threats cannot be confined to the regulation of information or the protection of technological infrastructures.

Instead, they require the development of cognitive capacities capable of preserving interpretative coherence, resisting manipulation, and maintaining decision autonomy under conditions of strategic influence. In this context, *cognitive resilience* becomes not only a complementary dimension of security, but a central epistemic mechanism for safeguarding the integrity of meaning-making processes in an increasingly contested cognitive domain.

The integration of Iu. Chifu's framework of cognitive-informational warfare further strengthens this analytical argument. Iu. Chifu and C. Grigore demonstrate that contemporary conflict has evolved into a form of full-spectrum warfare, in which cognitive and informational instruments are systematically employed to manipulate perceptions, distort reality, and influence decision-making processes [22, pp. 13-14]. These operations extend beyond traditional domains of conflict, targeting the reinterpretation of historical narratives, the manipulation of electoral processes, and the exploitation of social cleavages. However, while Iu. Chifu and C. Grigore's contribution is particularly strong in its descriptive and strategic dimensions; it does not fully elaborate the internal cognitive mechanisms of resistance. This reveals a significant epistemological gap: whereas Iu. Chifu explains how minds are manipulated, the present approach seeks to explain how they can resist such manipulation [23, pp. 47-53].

Accordingly, *cognitive resilience* can be understood as the defensive counterpart to cognitive-informational warfare. If the latter targets perception, interpretation, and decision-making, the former aims to preserve the integrity of these processes. In this sense, *cognitive resilience* constitutes a condition of democratic security, ensuring that decision-making remains autonomous and grounded in coherent interpretations of reality.

In conclusion, *cognitive resilience* should not be regarded as a mere extension of existing resilience frameworks, but rather as a distinct dimension of security, adapted to a strategic environment in which conflict is increasingly informational, manipulation is fundamentally cognitive, and vulnerability is epistemic in nature. Its conceptualisation enables the integration of cognitive processes into the analysis of contemporary security, providing both a strong theoretical foundation and a basis for the development of empirical instruments and policy responses. Presented perspectives collectively confirm that contemporary conflict increasingly unfolds within the cognitive domain, rendering the construction of meaning, the perception of reality, and the integrity of decision-making processes primary targets of strategic influence.

This transformation is consistent with insights from political psychology, which emphasise that international relations and foreign policy decisions are fundamentally shaped by how individuals perceive, interpret, feel about, and react to their environment [24, p. x]. Rather than acting as purely rational agents, decision-makers operate within cognitive and perceptual frameworks that structure their understanding of reality, thereby rendering perception itself a critical determinant of political and strategic outcomes. In this sense, security threats that target perception and cognition have the potential to influence not only individual behaviour but also state-level decision-making processes.

Further support for this perspective is provided by advances in cognitive science, particularly dual-process theories of cognition. Lodge, Taber, and Weber (2006) demonstrate that human cognition operates through both automatic and deliberative processes, with automatic responses emerging in milliseconds and preceding conscious reasoning [25, p. 12]. These automatic processes, rooted in associative memory structures and prior beliefs, strongly influence subsequent conscious judgments, evaluations, and decisions.

As a result, cognition is not neutral or purely rational, but inherently shaped by pre-existing cognitive and affective structures, making it particularly susceptible to manipulation in environments characterised by high informational density and strategic communication.

At the societal level, the vulnerability of cognitive processes is further amplified by the role of identity in structuring perception and political behaviour. Research on ideological polarisation shows that identity-based processes can operate independently of, and at times more powerfully than, issue-based reasoning. L. Mason demonstrates that ideological identities are rooted in dynamics of "inclusion and exclusion" [26, pp. 867-868], generating strong affective attachments and social divisions. These identity-driven dynamics reduce openness to alternative interpretations, reinforce cognitive rigidity, and increase susceptibility to manipulation and disinformation.

Taken together, these theoretical developments indicate that cognition has become a central domain of strategic competition. In this context, resilience must be reconceptualised to address not only systemic or institutional vulnerabilities but also cognitive ones. It is precisely within this analytical gap that *cognitive resilience emerges as a distinct conceptual category*.

Building on this theoretical framework, the following section examines how cognitive resilience operates within the EU security paradigm, particularly in relation to disinformation and cognitive vulnerability.

3. COGNITIVE RESILIENCE WITHIN THE EU SECURITY PARADIGM

3.1 Disinformation and cognitive vulnerability

The proliferation of disinformation within the European Union has exposed not only structural and informational vulnerabilities, but, more fundamentally, the fragility of cognitive systems underpinning democratic societies. Contemporary disinformation campaigns are no longer limited to the dissemination of false or misleading content; rather, they are strategically designed to exploit cognitive biases, emotional responses, and identity-based divisions, thereby reshaping how individuals perceive, interpret, and act upon political and social realities. As highlighted in the literature on online propaganda and disinformation, modern influence operations leverage digital ecosystems to manipulate perception and mobilize audiences through targeted messaging and algorithmic amplification.

A central mechanism through which disinformation operates is the systematic exploitation of cognitive biases. Research in political communication and security studies shows that individuals process information through heuristic and affective filters rather than through fully rational evaluation. In the contemporary information environment, campaigns of disinformation increasingly leverage cognitive vulnerabilities such as confirmation bias, selective exposure, and emotional salience to enhance the acceptance and diffusion of manipulated narratives [27]. This suggests that the effectiveness of disinformation lies not solely in the content itself, but in its alignment with pre-existing cognitive and emotional predispositions.

This perspective is further reinforced by empirical and theoretical work on cognitive biases in decision-making processes. C. Muntwiler identifies more than 180 distinct cognitive biases that may distort strategic judgment, demonstrating that decision-makers are systematically prone to errors rooted in both heuristic shortcuts and motivational factors, particularly under conditions of complexity and uncertainty [28, p. 32]. This extensive mapping of biases underscores the structural vulnerability of human cognition in environments saturated with competing and often conflicting information.

The impact of these biases is amplified by the dynamics of motivated reasoning. Ch. Taber and M. Lodge show that individuals tend to selectively accept information that confirms their prior beliefs while dismissing contradictory evidence, a phenomenon conceptualised as both confirmation bias and disconfirmation bias [29, pp. 755-756]. This process leads to attitude polarisation, whereby exposure to mixed information does not moderate opinions but instead reinforces pre-existing positions. In the context of disinformation, this implies that corrective information may not only fail to mitigate false beliefs but may inadvertently strengthen them, particularly among individuals with strongly held prior attitudes.

The vulnerability of cognitive systems is further intensified by the role of identity in structuring perception. Identity-based polarisation creates powerful in-group/out-group dynamics that influence how information is interpreted and evaluated. As L. Mason demonstrates, ideological identities function through dynamics of "inclusion and exclusion" [26, pp. 867-868], generating affective polarisation and reinforcing cognitive rigidity. This identity-driven filtering reduces openness to alternative perspectives and increases susceptibility to manipulation, particularly in highly polarised environments.

From the perspective of political psychology, these vulnerabilities extend beyond individual citizens to encompass political elites and institutional actors. Foreign policy decisions are shaped by how individuals perceive, interpret, feel about, and react to their environment [24, p. ix], rather than by objective assessments alone. This implies that disinformation has the potential to influence not only public opinion but also strategic decision-making processes at the highest levels of governance.

At the structural level, digital ecosystems significantly amplify these dynamics. Social media platforms enable the rapid dissemination, amplification, and personalisation of content, allowing both state and non-state actors to influence large audiences with unprecedented speed and precision. As J. Prier argues, contemporary information operations increasingly target people within a society, influencing their beliefs as well as behaviours, and diminishing trust in the government [30, p. 51]. By exploiting algorithmic dynamics and network effects, disinformation campaigns can artificially amplify specific narratives, generating the *illusion of consensus* and reinforcing pre-existing cognitive biases. This mechanism operates not merely at the level of information exposure, but at the level of *epistemic conditioning*, where repeated visibility and perceived popularity substitute for evidentiary validation.

Within the European Union, the policy response to disinformation has evolved significantly over the past decade, particularly through the development of a multidimensional regulatory and strategic framework. As P. Cesarini argues, the adoption of the Digital Services Act (DSA) in 2022 represents a major regulatory shift, requiring online platforms to identify and mitigate systemic risks associated with disinformation, while simultaneously balancing concerns related to freedom of expression, legal certainty, and proportionality [4, pp. 551-575]. This regulatory approach reflects a broader European effort to address disinformation not only through content moderation, but also through structural mechanisms such as transparency requirements, risk assessment obligations, and co-regulatory instruments. Complementary initiatives, including the European Media Freedom Act and the European Digital Media Observatory, further aim to strengthen media resilience, enhance information integrity, and promote societal awareness in the face of foreign information manipulation and interference.

These developments are consistent with the broader strategic orientation of the European Union, which increasingly emphasises resilience as a core principle of security governance. EU policy documents highlight the need to counter hybrid threats, including disinformation, through coordinated, whole-of-society approaches that integrate institutional, technological, and societal dimensions.

In this context, the management of information environments, the protection of democratic processes, and the strengthening of societal resilience have become central priorities within the EU's security architecture.

However, despite these advances, the EU's approach remains predominantly oriented toward the regulation and governance of information environments, rather than toward the cognitive mechanisms that enable disinformation to be effective. While regulatory frameworks such as the DSA can limit the spread and amplification of harmful content, they do not fully address the underlying cognitive predispositions, such as biases, motivated reasoning, and identity-based filtering, that shape how information is perceived, interpreted, and internalised. As a result, existing strategies risk remaining reactive and only partially adaptive to the evolving nature of cognitive warfare, which operates primarily at the level of perception, meaning-making, and decision-making.

In this context, the concept of *cognitive resilience* becomes essential. *Cognitive resilience* may be understood as the capacity of individuals and societies to resist manipulation, critically evaluate information, and maintain coherent interpretative frameworks under conditions of informational pressure. It functions as an epistemic filtering mechanism, enabling actors to navigate complex and often conflicting information environments without succumbing to cognitive distortion or strategic influence.

At the same time, the development of *cognitive resilience* is contingent upon broader societal and institutional conditions. Civil society plays an important role in fostering media literacy, critical thinking, and pluralistic information ecosystems. However, as I.F. Ceusan, M. Costea, S. Costea highlight, the effectiveness of such efforts depends significantly on levels of institutional support and public trust, which vary across European contexts [31, p. 74]. In environments characterised by low trust and high polarisation, individuals are less receptive to corrective information and more likely to rely on identity-based interpretations, thereby limiting the effectiveness of resilience-building initiatives.

In synthesis, the proliferation of disinformation within the European Union reveals a structural vulnerability at the level of cognition. Disinformation exploits cognitive biases, identity dynamics, and digitally mediated amplification mechanisms to reshape perception and behaviour, thereby challenging traditional, information-centric approaches to security. Addressing these challenges requires a gradual shift toward a cognitive paradigm, in which the development of *cognitive resilience* complements existing regulatory and institutional measures. Strengthening the capacity of individuals and societies to process, interpret, and critically engage with information thus emerges as a necessary condition for enhancing the European Union's ability to respond effectively to the evolving dynamics of cognitive warfare.

3.2 Cognitive resilience as a strategic capability in the European Union

The increasing centrality of cognitive vulnerability within the European Union has catalysed a gradual but significant shift from reactive counter-disinformation measures toward a more proactive and systemic approach centred on resilience. Within this evolving paradigm, *cognitive resilience* emerges not merely as a defensive response to informational threats, but as a *strategic capability* embedded within the broader architecture of European security and defence.

This transformation is closely linked to the evolution of the European Union's strategic thinking, particularly as reflected in the transition from the *EU Global Strategy (2016)* to the *Strategic Compass (2022).* The Global Strategy explicitly recognises that internal and external security are ever more intertwined and identifies state and societal resilience as a core priority of EU external action [10, p. 14].

This formulation marks a critical departure from traditional security paradigms by acknowledging that vulnerabilities originate not only in external threats but also within internal societal structures.

The Strategic Compass further operationalises this shift by establishing resilience as a central objective of EU security policy. As outlined in its implementation framework, the Compass constitutes an actionable framework for the EU's security and defence until 2030, aiming to increase the EU's resilience, strengthen defence capabilities and enhance its ability to act [32, p. 1]. Importantly, the document situates resilience within the context of hybrid and cyber threats, recognising that contemporary security challenges extend into the informational and cognitive domains.

The strategic relevance of this transformation is reinforced by the European External Action Service's analysis of *Foreign Information Manipulation and Interference (FIMI)*. The EEAS report explicitly states that today's wars are not only fought with tanks and drones but with lies and algorithms, emphasizing that the information space is a frontline in the fight for democracy [32, p. 2]. Furthermore, FIMI operations are described as deliberate attempts to manipulate citizens in order to shape views, political choices and ultimately the way we vote (EEAS, 2026, p. 2) [32, p. 2]. These formulations clearly indicate that contemporary threats directly target cognitive processes, including perception, judgment, and decision-making.

Within this context, *cognitive resilience* must be understood as a *core enabling capability* that allows the European Union to withstand and counter such forms of influence. Unlike regulatory or technological responses, which primarily address the supply of information, *cognitive resilience* focuses on the *interpretative dimension of security*, namely how individuals and societies process and internalize information.

The Strategic Compass implicitly supports this perspective through its emphasis on resilience against hybrid threats and its call for coordinated action across multiple domains. However, critical assessments highlight important limitations. The European Economic and Social Committee notes that the Strategic Compass does not sufficiently take into account the role European civil society can and must play in order to attain greater resilience against hybrid attacks and the systematic undermining of cohesion [34, p. 20]. This observation is particularly relevant, as *cognitive resilience* is fundamentally dependent on societal factors such as trust, cohesion, and civic engagement.

This limitation is further confirmed by recent analyses of EU cognitive security frameworks. L. Ariton demonstrates that, despite increasing institutional awareness reflected in instruments such as the Strategic Compass and the Digital Services Act, the European Union's response to cognitive warfare remains fragmented, characterised by weak civil-military coordination and persistent vulnerability to AI-driven disinformation [35, pp. 1-2]. These findings reinforce the argument that existing EU approaches are structurally insufficient to address the cognitive dimension of contemporary threats. From an operational perspective, *cognitive resilience* can be conceptualised as a *multi-layered strategic capability*, encompassing three interdependent levels.

At the *individual level*, *cognitive resilience* involves the ability to critically evaluate information, recognize cognitive biases, and engage in reflective reasoning. As demonstrated by Ch. Taber and M. Lodge, individuals exhibit strong tendencies toward confirmation bias and motivated reasoning, selectively accepting information that aligns with prior beliefs while rejecting contradictory evidence [29, pp. 755-756]. Moreover, automatic cognitive processes shape perception prior to conscious deliberation, making individuals particularly vulnerable to emotionally charged and identity-relevant information [25, p. 12].

At the *societal level*, *cognitive resilience* is shaped by the structure of the information environment, as well as by social cohesion and identity dynamics. The EEAS report highlights that FIMI operations systematically exploit divisions within societies and increasingly rely on artificial intelligence, which enables the mass production of manipulative content at speed, scale and low cost [32, p. 2]. These developments amplify cognitive vulnerability by overwhelming individuals with information and reinforcing heuristic processing.

At the *institutional level*, *cognitive resilience* depends on governance capacity, strategic communication, and the credibility of public institutions. The EU's capability development framework underscores the need to adapt to emerging threats by integrating technological, cyber, and informational dimensions into defence planning. As noted in the EU Capability Development Priorities, evolving security challenges require the development of capabilities that address both current operational needs and future threat environments [36, p. 4].

All presented levels interact dynamically, forming a complex adaptive system in which *cognitive resilience* is continuously reinforced or undermined. A weak institutional trust can exacerbate societal polarization, thereby increasing individual susceptibility to disinformation. Conversely, strong institutional credibility and effective communication can enhance both societal cohesion and individual cognitive capacities.

Importantly, *cognitive resilience* also contributes to the European Union's capacity to act as a credible security actor in an increasingly complex strategic environment. The Strategic Compass establishes an actionable framework aimed at enhancing the EU's resilience, strengthening security and defence partnerships, and increasing its ability to act and respond to crises [32, pp.1-2]. These objectives are further reinforced by broader EU policy commitments, such as the Versailles Declaration, which emphasises the need for the Union to take more responsibility for its own security and to increase its capacity to act autonomously in the face of evolving geopolitical challenges. Within this evolving strategic framework, the credibility of the EU as a security actor depends not only on material capabilities and institutional coordination, but also on its ability to maintain internal coherence, safeguard decision-making processes, and effectively shape and sustain strategic narratives. In this sense, *cognitive resilience* supports both the defensive and proactive dimensions of EU security, enabling the Union to resist external manipulation while preserving the integrity of its strategic communication and policy responses.

Ultimately, the integration of *cognitive resilience* into the European Union's security paradigm reflects a broader transformation in the ontology of security. Security is no longer defined solely in terms of territorial defence or institutional robustness, but increasingly in terms of the capacity to preserve cognitive autonomy and epistemic coherence in the face of strategic manipulation. *Cognitive resilience* thus emerges as a *strategic enabler*, bridging the gap between traditional security approaches and the realities of cognitive warfare.

In synthesis, the development of *cognitive resilience* as a strategic capability represents a necessary evolution of the European Union's response to disinformation, hybrid threats, and cognitive warfare. By shifting the focus from reactive regulation to proactive capacity-building, the EU can enhance its ability to withstand and adapt to cognitive challenges. However, achieving this objective requires a coherent and integrated approach that combines regulatory frameworks, institutional reform, societal engagement, and technological adaptation. Only through such a comprehensive strategy can *cognitive resilience* become a sustainable and effective pillar of European security.

4. DISCUSSION AND POLICY IMPLICATIONS

The integration of *cognitive resilience* into the European Union's security architecture must be analysed in the context of a rapidly evolving threat environment, in which information manipulation has become a central instrument of geopolitical competition. Empirical evidence provided by successive European External Action Service (EEAS) reports on Foreign Information Manipulation and Interference (FIMI) indicates that contemporary threats extend beyond the informational domain and increasingly operate at the level of perception, interpretation, and decision-making processes. The first EEAS report defines FIMI as a manipulative in character, conducted in an intentional and coordinated manner, capable of undermining democratic processes and societal stability [37, p. 4]. Subsequent analyses further emphasise that foreign actors systematically attempt to manipulate facts, to confuse, sow division, fear and hatred [38, p. 2], highlighting the strategic use of information to influence societal dynamics.

By 2025, the EEAS explicitly characterises the information space as a *geopolitical battleground*, where actors seek to manipulate public opinion, fuel polarisation, and interfere with democratic processes [39, p. 2]. This evolution is reinforced in the 2026 report, which notes that today's wars are not only fought with tanks and drones but with lies and algorithms, aiming to shape our views, political choices and ultimately the way we vote [32, p. 2].

At the *policy level*, these findings reveal a structural limitation in the current EU approach. While the Strategic Compass recognises the need to counter hybrid threats, disinformation, and cyber-attacks, and emphasises situational awareness, partnerships, and coordinated responses [40, pp. 5-6], it does not explicitly conceptualise *cognitive resilience* as a distinct strategic pillar. Similarly, the EEAS FIMI framework integrates analytical and operational tools for detection, attribution, and disruption [38, p. 15], but remains primarily focused on managing information flows rather than strengthening cognitive capacities.

This imbalance reflects a broader tendency within EU policy to prioritise external threat mitigation over internal cognitive preparedness. As EEAS reports indicate, FIMI operations are effective in part because they exploit pre-existing vulnerabilities within societies, including polarisation, fragmented information environments, and broader trust-related dynamics [39, p. 2]. Without addressing these underlying mechanisms, regulatory and strategic responses risk remaining reactive and incomplete.

In parallel with these policy developments, recent empirical research has attempted to operationalise *cognitive resilience* through composite indicators capturing institutional quality, digital infrastructure, and socio-economic variables [41]. While such approaches provide valuable comparative insights into the structural conditions associated with resilience across European states, they risk conflating *cognitive resilience* with broader systemic or societal resilience. In particular, these models do not directly capture the cognitive mechanisms, such as perception, interpretation, and judgment, that constitute the core focus of the present study. As a result, they offer only an indirect approximation of *cognitive resilience*, highlighting the need for more conceptually grounded and cognitively sensitive frameworks.

This assessment is consistent with recent conceptual work that positions resilience as a strategic pillar of cognitive security [3]. While such approaches highlight the growing recognition of resilience within contemporary security thinking, they do not fully specify the cognitive mechanisms through which perception, interpretation, and decision-making are affected under conditions of information manipulation.

At the *educational level*, the Digital Education Action Plan (2021-2027) provides an important, albeit partial, foundation for the development of *cognitive resilience*. The Action Plan emphasises the need to enhance digital skills, including digital literacy and the capacity to tackle disinformation [42, p. 2]. However, its focus remains predominantly on technical and informational competences, without fully integrating insights from cognitive psychology regarding biases, heuristic processing, and identity-based reasoning. This limitation is significant, as individuals do not process information in a purely rational manner. As demonstrated by Ch. Taber and M. Lodge, individuals exhibit motivated reasoning, selectively accepting information that confirms prior beliefs [29, pp. 755-756]. Similarly, M. Lodge, Ch. Taber, and C. Weber show that automatic affective processes shape perception prior to conscious deliberation [25, p. 12]. Consequently, educational strategies must move beyond traditional media literacy and incorporate metacognitive competencies, including awareness of cognitive biases and the mechanisms of manipulation.

At the *technological level*, EEAS analyses highlight the increasing role of artificial intelligence in amplifying FIMI operations. The 2026 report notes that AI enables the large-scale and low-cost production of manipulative content, including synthetic images and videos [32, p. 2]. This development significantly increases the complexity of the threat environment, as the distinction between authentic and manipulated content becomes increasingly blurred.

At the *societal level*, the implications of FIMI are particularly profound. EEAS reports emphasise that such operations aim to sow division, fear and hatred and undermine democratic cohesion [38, p. 2]. By exploiting existing social cleavages, FIMI not only distorts information but also weakens the foundations of democratic governance. As L. Mason demonstrates, identity-based polarisation reduces openness to alternative viewpoints and reinforces group-based interpretations of reality, thereby amplifying cognitive vulnerability [26, pp. 867-868].

Taken together, these findings suggest that contemporary security threats increasingly operate through cognitive pathways, affecting how individuals and societies perceive, interpret, and respond to information. In this context, *cognitive resilience* emerges not merely as an auxiliary capacity, but as a necessary complement to existing regulatory and strategic approaches.

5. CONCLUSIONS

The present study set out to examine whether *cognitive resilience* can be conceptualised as a distinct dimension of European Union security, or whether it remains subsumed within broader resilience frameworks. The findings provide strong theoretical and empirical grounds for advancing *cognitive resilience* as an *autonomous, analytically robust, and operationally relevant construct*, essential for understanding and responding to the transformation of the contemporary security environment.

First, the analysis indicates that the evolution of hybrid threats, disinformation campaigns, and cognitive warfare has altered the ontology of security. No longer confined to territorial defence or institutional stability, security increasingly unfolds within the cognitive domain, where perception, interpretation, and belief formation become strategic targets. As the authors elucidate, contemporary influence operations are designed not merely to distort information, but to reshape how individuals and societies construct reality, thereby influencing decision-making processes at both micro and macro levels. This shift necessitates a security reconceptualisation that explicitly incorporates the protection of cognitive processes.

Second, the study establishes that existing resilience frameworks, whether psychological, societal, or informational, are insufficient to capture the specificity of cognitive vulnerability. While each of these constructs addresses important aspects of adaptation and recovery, none adequately explains the mechanisms through which cognition itself is targeted and manipulated. *Cognitive resilience* fills this conceptual gap by focusing on the integrity, adaptability, and protection of meaning-making processes. In doing so, it introduces an epistemic dimension to security studies, repositioning cognition as both a site of vulnerability and a strategic resource.

Third, the authors advance a coherent theoretical framework for understanding *cognitive resilience* as a *multi-level and multidimensional capacity*, operating across individual, societal, and institutional domains. This framework highlights the dynamic interaction between cognitive biases, identity-based processes, information ecosystems, and governance structures, demonstrating that resilience is not a static attribute but a complex adaptive system. Importantly, this perspective allows for the integration of insights from cognitive psychology, political science, and security studies into a unified analytical model.

Fourth, the findings underscore the inadequacy of current European Union policy frameworks in addressing cognitive threats in a systematic manner. Although significant progress has been made through instruments such as the Strategic Compass, the Digital Services Act, and the FIMI response mechanisms, these approaches remain predominantly focused on regulating information flows and countering external actors. As the analysis indicates, such measures do not sufficiently address the internal cognitive mechanisms that enable disinformation to be effective. Consequently, the EU's response remains fragmented, lacking a coherent strategy that explicitly operationalises *cognitive resilience* as a core component of security policy.

Fifth, the study contributes to the field by proposing an *operational definition of cognitive resilience*, thereby facilitating its empirical measurement and comparative analysis. By identifying key dimensions, such as cognitive filtering capacity, interpretative coherence, adaptive flexibility, and epistemic trust, the study provides a foundation for the development of quantitative instruments and analytical models, including SEM-based approaches. This operationalisation represents a critical step toward bridging the gap between conceptual theory and empirical research.

Finally, the integration of *cognitive resilience* into the European security paradigm has significant policy implications. It requires a shift from reactive and fragmented approaches toward a *proactive, systemic, and interdisciplinary strategy*, encompassing policy design, education, technological innovation, and societal engagement. *Cognitive resilience* must be recognised as a strategic capability, essential for safeguarding democratic processes, maintaining social cohesion, and ensuring the autonomy of decision-making in an increasingly contested information environment.

In conclusion, *cognitive resilience* should not be regarded as a derivative or auxiliary concept, but as a *new dimension of security*, reflecting the realities of a strategic environment in which conflict is increasingly cognitive, manipulation is epistemic, and vulnerability resides in the processes through which reality is constructed and understood. By advancing this conceptualisation, the study not only contributes to the theoretical consolidation of security studies but also provides a framework for future research and policy development aimed at strengthening the European Union's capacity to navigate the challenges of cognitive warfare.

This study is subject to several limitations that should be acknowledged. First, the research is primarily conceptual and theory-building in nature, relying on qualitative analysis and theoretical meta-synthesis rather than on empirical validation.

As such, while it advances a coherent analytical framework for *cognitive resilience*, it does not test this construct through quantitative or experimental methods. Second, the operationalisation of *cognitive resilience* proposed in this study remains at a preliminary stage, requiring further refinement and empirical verification through future research, particularly in the development of measurable indicators and comparative models. Third, the analysis is largely focused on the European Union context, which may limit the generalisability of findings to other geopolitical settings characterised by different institutional, cultural, and informational dynamics.

REFERENCES

[1] C. Deppe, G.S. Schaal, Cognitive warfare: a conceptual analysis of the NATO ACT cognitive warfare exploratory concept, *Frontiers in Big Data*, *7*, 2024, 1452129;

[2] S.L. Vériter, C. Bjola, J.A. Koops, Tackling COVID-19 disinformation: internal and external challenges for the European Union, *The Hague Journal of Diplomacy*, *15* (4), pp. 569-582, 2020;

[3] M.A. Siewier, Resilience as a Strategic Pillar of Cognitive Security, *Humanities and Social Sciences*, *32*(4), pp. 169-183, 2025, https://doi.org/10.7862/rz.2025.hss.50;

[4] P. Cesarini, The EU Policy Framework to Counter Disinformation: Enabler or Inhibitor of Freedom of Expression?, in Ginsborg, L., Gori, P. (eds) *Disinformation: A Multi-Disciplinary Analysis*. Springer, Cham, pp. 551-575, 2026, https://doi.org/10.1007/978-3-032-00480-2_28;

[5] M. Wigell, H. Mikkola, T. Juntunen, 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 (pdf), 10, 379, 2021;

[6] E. Akıllı, Theoretical Foundations of Cognitive Diplomacy. In: *Cognitive Diplomacy and Digital Autonomy: Statecraft in the Age of Artificial Intelligence*. Palgrave Macmillan, Cham, pp. 185-197, 2025, https://doi.org/10.1007/978-3-032-04470-9_11;

[7] A. Romanishyn, O. Malytska, O., V. Goncharuk, AI-driven disinformation: policy recommendations for democratic resilience, *Frontiers in Artificial Intelligence*, 8, 2025, 1569115;

[8] T. Singh, Cognitive Warfare and Fake News in the Post-Truth Era, in *Digital Psychological Warfare: Weaponisation of Digital Platforms*, Palgrave Macmillan, Cham: Springer Nature Switzerland, pp. 45-63, 2026, https://doi.org/10.1007/978-3-032-15294-7_3;

[9] H.R. Heinimann, K. Hatfield, 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, 2017, https://doi.org/10.1007/978-94-024-1123-2_5;

[10] *A Global Strategy for the European Union's Foreign and Security Policy*, 2016;

[11] C.S. Holling, Resilience and stability of ecological systems, *Annual Review of Ecology and Systematics*, Vol. 4, November, pp. 1-23, 1973;

[12] F.S. Brand, K. Jax, Focusing the meaning (s) of resilience: resilience as a descriptive concept and a boundary object, *Ecology and society*, *12*(1), 23, 2007, [online] URL: http://www.ecologyandsociety.org/vol12/iss1/art23/;

[13] M. Rutter, Psychosocial Resilience and Protective Mechanisms, *Am J Orthopsychiatry*, July 57(3), pp. 316-331, 1987, doi:10.1111/j.1939-0025.1987.tb03541.x. PMID: 3303954;

[14] A. S. Masten, Ordinary magic: Resilience processes in development, *American psychologist*, 56.3, 227, 2001;

[15] G.A. Bonanno, Loss, trauma, and human resilience: have we underestimated the human capacity to thrive after extremely aversive events? *American psychologist*, *59*(1), 20, 2004;

[16] W.N. Adger, Social and ecological resilience: are they related?, *Progress in human geography*, *24*(3), pp. 347-364, 2000.

[17] F.H. Norris, S.P. Stevens, B. Pfefferbaum, K.F. Wyche, R.L. Pfefferbaum, Community resilience as a metaphor, theory, set of capacities, and strategy for disaster readiness, *American journal of community psychology*, *41*(1), pp. 127-150, 2008;

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

[19] Y. R. Masakowski, J.M. Blatny (eds.) *Mitigating and Responding to Cognitive Warfare (Atténuer et répondre à la guerre cognitive)*, NATO STO, 2023;

[20] B. Claverie, La guerre cognitive de bas niveau: la guerre des cerveaux, *Ingénierie cognitique*, 2024;
[21] B. Claverie, B. Prébot, La guerre cognitive de bas niveau: la guerre des cerveaux, *Ingénierie cognitique*, 7 (1), pp. 67-75, 2024, doi:10.21494/ISTE.OP.2024.1091*;*
[22] I. Chifu, C. Grigore, Full-spectrum warfare. From broadening the instruments to thinking the unthinkable, in Chifu, Iulian, Mârzac, Elena, Konstantinova Vira (eds.), *Cognitive-Informational Warfare in the Romania - Republic of Moldova - Ukraine Trilateral*. RAO Bucharest, pp. 13-46, 2025;
[23] I. Chifu, Conceptualization and epistemological evaluation: the cognitive warfare, in Chifu, Iulian, Mârzac, Elena, Konstantinova Vira (eds.), *Cognitive-Informational Warfare in the Romania - Republic of Moldova - Ukraine Trilateral*. RAO Bucharest, pp. 47-72, 2025;
[24] E. Singer, V. M. Hudson, *Political psychology and foreign policy*, Routledge, 2020;
[25] M. Lodge, C. Taber, Christopher Weber, First Steps Toward a Dual-Process Accessibility Model of Political Beliefs, Attitudes, and Behavior, in Redlawsk, D.P. (eds) *Feeling Politics.* Palgrave Macmillan, New York, 2006. https://doi.org/10.1057/9781403983114_2;
[26] L. Mason, Ideologues without issues: The polarizing consequences of ideological identities, *Public Opinion Quarterly*, *82*(S1), pp. 866-887, 2018;
[27] M. Gregor, P. Mlejnková, *Challenging Online Propaganda and Disinformation in the 21st Century*, Palgrave Macmillan, 2021;
[28] C. Muntwiler, *Cognitive biases and debiasing in strategic decision making*, Doctoral dissertation, Universität St. Gallen, 2023;
[29] C.S. Taber, Milton Lodge, Motivated Skepticism in the Evaluation of Political Beliefs, *American Journal of Political Science*, vol. 50, issue 3, pp. 755-769, 2006, doi:10.1111/j.1540-5907.2006.00214.x;
[30] J. Prier, Commanding the trend: social media as information warfare, in *Information warfare in the age of cyber conflict*, Routledge, pp. 88-103, 2020;
[31] I.F. Ceusan, M. Costea, S. Costea, The Role of Civil Society in Fighting Disinformation: Successes, Failures, and Future Directions in Romania in the EU Context, *Europolity: Continuity & Change Eur. Governance*, *19*, 71, 2025;
[32] S. Clapp, *Implementation of the Strategic Compass: Opportunities, challenges and timelines*, Brussels, 2022;
[33] European External Action Service, *4th EEAS Report on Foreign Information Manipulation and Interference Threats*, March 2026, [online], https://www.eeas.europa.eu/eeas/4th-eeas-annual-report-foreign-information-manipulation-and-interference-threats_en (25.04.2026);
[34] Opinion of the European Economic and Social Committee on 'The EU Strategic Compass' (own-initiative opinion) (OJ C, C/140, 21.04.2023, CELEX: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022IE4219. 25.04.2026);
[35] L. Ariton, L. (2025). Cognitive warfare in the digital age: Implications for EU security policy. In *International conference KNOWLEDGE-BASED ORGANIZATION*, 31, vol. 2, pp. 1-9, doi:10.2478/kbo-2025;
[36] European Defence Agency, The 2023 EU Capability Development Priorities, Publications Office of the European Union, 2023, https://data.europa.eu/doi/10.2836/229505;
[37] European External Action Service, *1st EEAS Report on Foreign Information Manipulation and Interference Threats, Towards a framework for networked defence*, February 2023, [online] https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en. (25.04.2026);
[38] European External Action Service, *2nd EEAS Report on Foreign Information Manipulation and Interference (FIMI) Threats*, January 2024, [online] https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en. (25.04.2026);
[39] European External Action Service, 3rd EEAS report on Foreign Information Manipulation and Interference Threats, March 2025, [online], https://euneighbourseast.eu/news/publications/third-eeas-report-on-foreign-information-manipulation-and-interference-threats/. (25.04.2026);
[40] J.A Koops, R. Pacheco Pardo, *The strategic compass: implementing the partnership dimension in the area of security and defence*, 2023;
[41] C.M. Dalban, E. Coman, V. Bătrânu-Pințea, M. Anton, I. Para, L.I. Mazuru, Mapping European Countries' Resilience to Cognitive Warfare, *Administrative Sciences*, *16*(3), 160, 2026, https://doi.org/10.3390/admsci16030160;
[42] Digital Education Action Plan 2021-2027. Resetting education and training for the digital age, 2020, [online], https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0624, (25.04.2026).