

# Cognitive Dimension of the Information Environment and Civil Population Resilience: The Case of Slovakia

Tatiana FÁBRYOVÁ\*, Vladimír ZVEREC, Ivan MAJCHÚT, Peter GEREC

*Security and Defence Department, Armed Forces Academy of Gen. M. R. Štefánik, Demänová 393, 031 01 Liptovský Mikuláš, Slovakia*

Correspondence: \*[fabryova.tatiana@gmail.com](mailto:fabryova.tatiana@gmail.com)

## Abstract

This paper analyses the cognitive vulnerabilities of the Slovak information environment and identifies mechanisms through which adversarial actors exploit societal fractures to undermine national strategic resilience. The research employs a theoretical-empirical analysis, integrating NATO doctrinal frameworks with psychological concepts and current sociological data on public trust in Slovakia. The findings reveal significant cognitive lability regarding strategic alignment and demonstrate how horizontal mistrust facilitates strategic paralysis. Based on these findings, the authors identify the process of the Preparation of the Population for State Defence as one of the strategic tools for building cognitive resilience. The study provides an original synthesis of cognitive warfare theory and empirical facts, establishing cognitive sovereignty as a cornerstone of modern national security.

**KEY WORDS:** *cognitive dimension, information environment, psychological operations, cognitive resilience of civil population.*

**Citation:** Fábryová, T.; Zverec, V.; Majchút, I.; Gerc. P. Cognitive Dimension of the Information Environment and Civil Population Resilience: The Case of Slovakia. In Proceedings of the Challenges to National Defence in Contemporary Geopolitical Situation, Brno, Czech Republic, 7-10 September 2026. ISSN 2538-8959, <https://doi.org/10.47459/cndcgs.2026.54>

## 1. Introduction

The current development of human civilization is very dynamic, changeable, unstable and in recent years highly turbulent [1]. In several regions of the world, there are sudden changes in the security situation and an increase in military and non-military security threats [2]. At the same time, we are currently witnessing a fundamental shift in global conflict, where traditional kinetic operations are becoming secondary to battles occurring within the information environment. The modern battlefield is no longer defined solely by geographical borders, but primarily by the ability of actors to influence the perception of reality, attitudes, and decision-making processes of target audiences. The information environment has thus emerged as a decisive strategic space where state and non-state actors leverage advanced technologies and psychological mechanisms to achieve political and security objectives without the necessity of open military aggression. Understanding these dynamics is therefore no longer an academic exercise, but a vital prerequisite for ensuring the strategic sovereignty and resilience of the state in the digital age.

A key element of this environment is the cognitive dimension - the domain of human thought, emotion, and belief. It is precisely this dimension that represents the most critical point of vulnerability in modern society. In the context of cognitive warfare, the very integrity of an individual's perception becomes the target of attack. Adversarial disinformation [3], sophisticated propaganda<sup>1</sup>, and manipulative narratives [4] are purposefully designed to exploit inherent psychological weaknesses, deepen social polarization, and ultimately erode trust in state institutions. The Slovak Republic represents a specific case of a country facing intense pressure within the cognitive space. The accumulation of historical sentiments, low institutional trust, and a high degree of susceptibility to alternative narratives creates an environment where adversarial operations can achieve strategic effects with minimal effort. This vulnerability directly threatens the overall resilience of the population and the state's operational capacity in crisis situations.

This paper explores the dynamics of the information environment with a focus on its cognitive component. The aim is to analyse how theoretical concepts of cognitive lability and psychological manipulation translate into the practical

reality of the Slovak security context. Understanding these mechanisms is an essential prerequisite for building effective cognitive defence and ensuring the strategic sovereignty of the state in the digital age.

## 2. Theoretical Foundations of the Information Environment

The contemporary security environment is increasingly influenced by the dynamics of the information environment, where technological, social, and psychological factors converge to shape the behaviour of both individuals and society. The information environment has emerged as a significant arena for the strategic activities of state and non-state actors who, through information and psychological operations, seek to manipulate the perception of reality, attitudes, and decision-making processes of target audiences [3]. Consequently, for the analysis of current security threats, it is essential to theoretically ground the fundamental concepts related to the information environment, with particular attention devoted to the cognitive dimension, which represents the critical domain where the ultimate effects of information activities manifest. Therefore, this chapter presents the theoretical foundations of the information environment and elucidates the significance of the cognitive dimension within the context of information [4] and psychological [4] operations [5–7].

### 2.1. Definition and Conceptualization of the Information Environment

Widespread accessibility of information technologies has expanded the operational space for manipulative information [8] and influence [8] activities of both military and non-military origin, posing a severe challenge to communal cohesion and the integrity of society and the state. These activities represent a demonstrable long-term trend that fundamentally shapes the contemporary information and security environment [9,10]. The *information environment* is a diverse global space comprising physical, virtual, and cognitive dimensions. It is an environment where individuals and automated systems consciously or unconsciously orient themselves, observe, make decisions, and act based on data, information, knowledge, and experience. This interconnected global information environment has fundamentally transformed how people communicate, share data and information, and perceive media [11,8]. Within the context of North Atlantic Treaty Organization (NATO), the information environment is defined as: “an environment comprised of the information itself, the individuals, organizations and systems that receive, process and convey information, and the cognitive, virtual and physical space in which this occurs” [4].

Crucial significance of globally distributed information, the speed of its communication, the role of the media, and the reliability of information systems have created a situation where no decision or measure can be taken without considering its potential impact on the information environment [12]. The information environment can rapidly and massively influence anyone at any level. These factors both threaten and enable the exploitation of societal vulnerabilities [13].

### 2.2. Three Dimensions of Information Environment

Structurally, the information environment is divided into three core dimensions: cognitive, virtual, and physical. As illustrated in Figure 1.

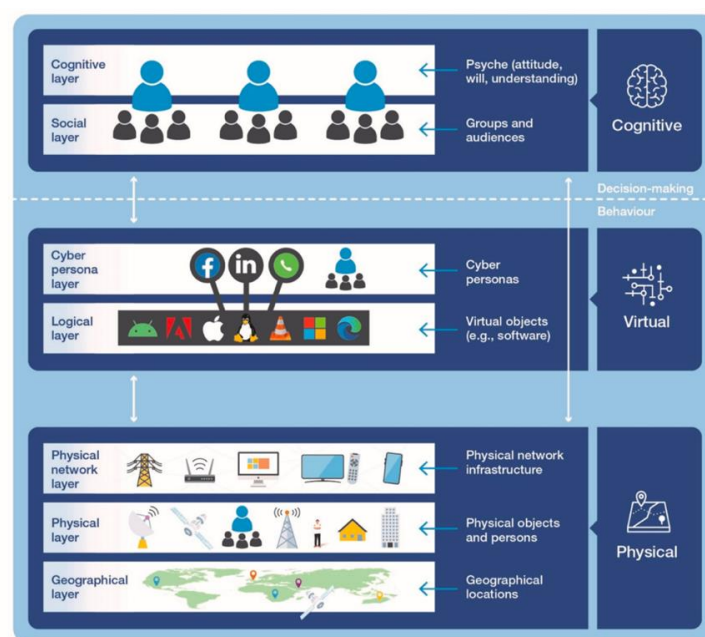


Fig. 1 Information Environment [8]

These dimensions are further categorized into seven distinct layers, allowing for a more precise analysis of functions that extend beyond mere communication and the military means used to induce changes in attitudes and behaviour. Interconnectedness between these dimensions and their respective layers expands the potential for identifying targets while simultaneously revealing the interrelated aspects of the information space. By conceptualizing individual layers (apart from the cognitive one) as potential communication channels, actors can broaden not only the range of possible targets but also the repertoire of instruments available to achieve desired strategic outcomes [8].

### 2.2.1. Cognitive Dimension

As the decisive domain of the information environment, this dimension is where cognitive effects directly influence individual thinking, and consequently, subsequent behaviour and decisions. Structurally, it comprises two distinct layers: cognitive and social. Ultimately, this dimension is shaped by the cumulative impact of all actions occurring within the physical and virtual dimensions [8,6,14,15].

Within the *cognitive layer*, individuals process and interpret information internally, without any external manifestation. Being inherently intangible and unobservable, this layer encompasses the fundamental will, cohesion, and perceptions of the audience, as well as their beliefs, values, and strategic goals [8,6,16,17].

Shifted to the *social layer*, the focus moves to how individual behaviour is shaped by the pressures of the socio-cultural environment. Here, social groups and cultural norms act as powerful filters for individual decision-making, including all forms of interaction within economic or political spheres. Furthermore, this layer serves as the primary domain for key influencers who possess significant outreach. In this context, planners must rigorously assess the credibility and reach of these actors to effectively sway specific audiences [8,17,18].

### 2.2.2. Virtual Dimension

Representing the digital space in which audiences interact, this dimension consists of two distinct layers: cyber persona and logical [8].

Within the *cyber persona* layer, the focus is on how individuals manifest themselves through online profiles and interactions with followers or subscribers. Modern actors in this space may operate under multiple identities, whether managed personally or generated through artificial intelligence. Beyond traditional physical means, key influencers leverage this specific layer to exert significant influence over their audiences [8,3,19].

Parallel to this, the *logical layer* serves as the functional environment where the processing, storage, and transmission of analogue and digital data occur. It acts as the virtual infrastructure supporting various dependencies, services, and resources utilized for data exchange, including social media platforms and file storage. Furthermore, this layer encompasses network configurations, data transfer protocols, domain names, and other electromagnetic processes. Operating almost entirely within the cyber domain, activities at this level can directly jeopardize the confidentiality, integrity, or availability of critical data [8,19].

### 2.2.3. Physical Dimension

Composed of geographic areas where audiences reside, this dimension includes all physical objects and the supporting infrastructure. It represents the space where physical activities occur and where individuals, nations, states, cultures, and societies interact. Structurally, it consists of three layers: the physical network, physical, and geographic layers [8,18].

First, the *physical network* layer represents the foundational infrastructure underpinning the virtual layers. Its primary function involves the transmission and reception of unstructured raw data between devices and physical transmission media. Included in this infrastructure is hardware that enables communication (such as radio towers, satellite transmitters, receivers, and converters) the components of which can be described in terms of network topology [8,20].

Second, the *physical layer* serves as the domain where audience interaction occurs, encompassing both technical-communication and human infrastructure. The latter includes physical areas that facilitate communication, such as marketplaces, meeting places, or places of worship. Within this specific context, words and images are categorized as physical information rather than virtual assets [8,18,20].

Finally, the *geographic layer* accounts for the impact of environmental conditions, such as population density and climate, on the methods through which the audience communicates [8].

## 2.3. Decisive Role of the Cognitive Dimension

Based on the characteristics, it can be concluded that the information environment constitutes a complex and dynamically interconnected system in which physical, virtual, and cognitive elements interact. While each dimension serves a specific function, their true significance is manifested primarily through their mutual interaction. Activities executed within the physical or virtual dimensions can, through various layers, induce effects [21] in the cognitive

dimension, which represents the domain where the perception, attitudes, and decision-making of individuals and social groups are formed [22,23].

Consequently, the cognitive dimension is regarded as the pivotal area where the ultimate effects of information and communication activities are realized. It is precisely the ability to influence how an audience interprets information that creates the preconditions for altering the behaviour or decision-making of target groups. Within the context of contemporary security threats, information and psychological operations are therefore increasingly directed toward this dimension, which has become the primary target of adversarial influence [8,24].

Accordingly, the following chapter will examine the evolution of these threats, moving from traditional psychological operations to the emerging concept of cognitive warfare. It will analyse the specific mechanisms through which adversaries exploit human psychological vulnerabilities to influence the perception, attitudes, and behaviour of the target audience.

### 3. From Psychological Operations to Cognitive Warfare

This chapter explores the mechanisms and evolution of influence operations, tracing their development from traditional psychological techniques to the advanced paradigm of cognitive warfare. By analysing how adversarial actors exploit human psychological vulnerabilities and leverage emerging technologies, it establishes a theoretical bridge between the structure of the information environment and its practical application in modern strategic conflicts. The following sections detail the transition from targeting individual perception to the systematic manipulation of societal cognitive processes.

#### 3.1. Mechanisms of Psychological Influence

The cognitive dimension represents the critical domain where the ultimate effects of information and psychological operations manifest. While individual activities may be executed through instruments in the physical or virtual dimensions of the information environment, their primary objective is to influence the manner in which individuals and social groups interpret information, form attitudes, and make decisions. In contemporary conflicts, increasing emphasis is placed on the significance of the cognitive dimension, where the human mind itself becomes the battlefield and the target of adversarial influence [20].

Psychological warfare [20] is arguably the most prevalent method of generating effects in and through social network media in contemporary conflicts, conducted by virtually all actors. Psychological warfare in and through social network media is aimed at the cognitive domain and is heavily based on human factors analysis [8] and target audience analysis [8]. It is fundamentally aimed at maintaining the support of the loyal, convincing the uncommitted, and undermining the opposition. This is achieved by influencing people's perception of ongoing events and, in turn, affecting their online and offline behaviour by leveraging emotional and logical arguments drawn from existing conversations and history, and by tapping into established narratives. This can be accomplished by informing audiences of facts, but it may also involve exposing the opposition's wrongdoings or embarrassing actions, influencing through specifically curated words and images (synchronized in time and space with other activities), and disseminating misleading or false information, including through outright deception [24,20].

The effectiveness of information and psychological operations within the cognitive dimension is predicated on the existence of inherent human *psychological* and *social vulnerabilities*. These vulnerabilities stem from the ways individuals process information, respond to emotional stimuli, and develop trust in information sources. Consequently, adversaries employ various mechanisms of psychological influence aimed at manipulating the perception of reality and shaping the attitudes of the target audience. Frequently utilized techniques include the repetitive dissemination of narratives, which, through systematic repetition, reinforces a specific interpretation of reality and gradually anchors it within public discourse [25,26].

The "*framing*" of information (the way in which data is presented and interpreted) also plays a significant role. The same event can be presented through different frameworks to support a specific interpretation or evaluation of the situation. This is closely related to selective information disclosure, where only certain facts or aspects of events are emphasized while others are intentionally omitted or marginalized. Such an approach can lead to a distorted perception of reality and influence the decision-making of both individuals and social groups [18].

Another technique employed in information operations is *information overload*, where the audience is exposed to an excessive volume of often contradictory information. In such an environment, it is challenging for individuals to navigate the information space and critically evaluate individual sources, which can lead to information fatigue, reduced analytical capacity, and an increased susceptibility to simplified or manipulative interpretations [13].

#### 3.2. Psychological Vulnerabilities and Cognitive Biases

Modern concepts of cognitive influence emphasize that the objective of such activities is to disrupt rational decision-making, exploit psychological weaknesses, and weaken societal resilience against manipulative narratives. Significant human vulnerabilities in the cognitive dimension primarily include *cognitive biases* that affect information interpretation. One of the most frequently exploited is confirmation bias, where individuals tend to seek out and accept

information that confirms their existing beliefs while ignoring contradictory data. Similarly, the *availability heuristic* [27] causes individuals to perceive information that is most frequently presented or easily accessible in the information space as more probable [14,15,28,22].

Emotional reactions, such as *fear*, *anger*, or *frustration*, also play a vital role, as they can diminish the capacity for critical evaluation while increasing susceptibility to manipulative narratives. Societal vulnerability can be further exacerbated by low levels of media and information literacy, which complicates the distinction between credible information and manipulative content [29].

A critical factor is also the decline in trust toward authorities and institutions, which creates a fertile environment for the spread of alternative and conspiracy narratives. In such an information environment, information and psychological operations can significantly sway the perception of reality and the decision-making of individuals and social groups [29]. The aim of such influence is to affect not only what people think but also how they interpret information and reach decisions, thereby shaping their behaviour in alignment with the actor's strategic goals. Successful operations in the cognitive dimension may manifest as the erosion of trust in state institutions, the deepening of societal polarization, or a reduced public willingness to support national defence and security measures [29].

It follows that understanding human psychological vulnerabilities within the cognitive dimension is essential for analysing contemporary information threats and constitutes a vital prerequisite for building societal resilience against manipulative information activities.

### **3.3. Cognitive Warfare: Paradigm Shift in Modern Conflict**

Cognitive warfare represents a paradigmatic shift in the conceptualization of modern conflict, moving beyond the mere control of information flow to the manipulation of the cognitive processes themselves. While traditional information operations focus on “what the audience thinks,” cognitive warfare aims to alter “how the audience thinks.” North Atlantic Treaty Organization (NATO) recognizes this evolution by defining the human mind as the sixth domain of operations, standing alongside land, maritime, air, space, and cyber [14].

The fundamental objective of cognitive warfare is to induce “cognitive paralysis,” disrupt social cohesion, and erode institutional trust. This is achieved through the systematic exploitation of human psychological vulnerabilities, such as cognitive biases and heuristics, which allow adversarial actors to bypass an individual’s rational filters [15,22].

The rapid advancement of Emerging and Disruptive Technologies, specifically Artificial Intelligence, Big Data, and neurosciences acts as a “force multiplier” for cognitive aggression. As noted in the NATO Chief Scientist Research Report, these technologies enable the delivery of highly personalized and manipulative content at an unprecedented scale and speed. This “weaponization” [3] of social sciences and technology creates a persistent state of “cognitive fog,” where the target audience finds it increasingly difficult to distinguish between manufactured narratives and reality [14].

### **3.4. Societal Impacts and Imperative of Resilience**

In the context of contemporary security, the distinction between peace and conflict becomes blurred. Cognitive warfare often operates in a “legal blind spot,” utilizing grey-zone tactics that do not trigger a conventional military response but significantly undermine national stability. The civilian population is the primary target of this approach. By fragmenting public opinion and fostering radicalization, an adversary can paralyze a state’s decision-making capacity without firing a single shot [5,16].

The Alliance’s resilience stems from a critical combination of civil preparedness and military capacity [24]. Cognitive resilience, therefore, is not merely a reactive posture but a dynamic capability of a societal system to absorb cognitive shocks and maintain the integrity of its decision-making processes. This requires a “whole-of-society approach” that integrates education, media literacy, and technological defence to safeguard the cognitive sovereignty of the population. As Claverie and du Cluzel emphasize, the main challenge is that cognitive warfare is essentially invisible. Its impact is often only recognized when it is too late to reverse the strategic damage. [6].

## **4. Practical Context: Vulnerabilities of the Slovak Information Environment**

The effectiveness of cognitive warfare is fundamentally predicated on the pre-existing vulnerabilities of the target audience. In the Slovak Republic, the transition from theoretical models to operational reality reveals a systemic susceptibility where cognitive attacks bypass institutional defences to target societal cohesion. This chapter analyses the specific “open doors” in the Slovak cognitive dimension, drawing on historical, psychological, and institutional factors.

### **4.1. Institutional Fragility and “Legal Blind Spot”**

As established in the Communication Strategy of the Ministry of Defence [9], the dissemination of harmful information in Slovakia is a dominant hybrid threat [30] aimed at undermining the pillars of statehood. From the perspective of cognitive warfare, this represents a strategic exploitation of a “functional blind spot.” When trust in public institutions and the democratic system is systematically eroded, the population loses its “cognitive armour” [29,9].

Adversarial actors (state and non-state) leverage this trust deficit to disrupt social consensus on Slovakia's Euro-Atlantic orientation. This is not merely propaganda [3]. It is a coordinated effort to paralyze the state's decision-making capacity by ensuring that no official narrative is perceived as credible by a significant portion of the population [31].

#### **4.2. Ideological Anchoring: Pan-Slavism and Historical Sentiments**

A key mechanism of cognitive warfare is the use of narrative anchoring [25]. In Slovakia, this is achieved by weaponizing historical and cultural ties to Russia. As noted by Mesežnikov [32], the idea of Pan-Slavism [33] and a romanticized view of the common Slavic past serve as a psychological foundation for pro-Russian narratives [32].

These narratives present Russia not as a geopolitical actor, but as a "moral authority" and a conservative alternative to a "decaying West" [34]. This ideological framing exploits the availability heuristic: people tend to accept information that resonates with their deeply rooted cultural identity, even if it contradicts current geopolitical facts [34].

#### **4.3. Psychological Mechanisms: Cognitive Dissonance and Hofstede's Dimensions**

The susceptibility of the Slovak population can be further explained through psychological frameworks. Analysis based on Hofstede's cultural dimensions [35] indicates that Slovak society places high value on power distance and traditionalism, traits that are often personified by authoritarian leadership models [36,26].

When faced with the reality of Russian aggression, many individuals experience cognitive dissonance [37]. To resolve the internal conflict between their positive image of Russia and the facts of the war, they turn to conspiratorial explanations that relativize the aggression. This psychological "defence mechanism" is strategically fuelled by adversarial cognitive operations, which provide the necessary "alternative facts" to maintain internal consistency [36,26].

#### **4.4. Tactical Execution: Information Saturation and "Cognitive Fog"**

The Slovak information environment is subjected to a state of information overload, orchestrated by a sophisticated network of actors, including the Russian Embassy in Bratislava, reportedly one of the most active in Europe [38]. By flooding social media with contradictory, emotionally charged, and "weaponized" information, these actors induce a state of *cognitive fog* [20,13].

This environment makes it impossible for the average citizen to perform a rational "OODA loop" (Observe-Orient-Decide-Act) [24]. Instead of critical evaluation, the audience falls back on reflexive emotional reactions (fear, anger, and a sense of threat) which are the ultimate goals of cognitive warfare [24,31].

### **5. Empirical Analysis of Cognitive Vulnerability and Strategic (In)resilience of the Slovak Republic in the Context of the Information Environment**

Following the theoretical framework of the information environment, the Slovak context serves as a prime case study of how interactions in the virtual and physical dimensions translate into concrete effects within the cognitive dimension. This chapter analyses how theoretically defined psychological vulnerabilities and mechanisms of cognitive warfare manifest in contemporary Slovak reality.

#### **5.1. Dynamics of Cognitive Lability and the Failure of Institutional Anchors**

When examining attitudes toward Slovakia's strategic alignment within transatlantic structures, a phenomenon of so-called *reactive cognitive mobility* can be identified. Empirical data from 2021-2025 reveal that Slovak society responds to external security stimuli with a high degree of lability. While there was a sharp surge in support for NATO membership immediately following the Russian invasion of Ukraine in 2022 (rising to 72%) [39], the subsequent two years have shown a significant regression toward pre-war levels (dropping back below 60%) [40].

From a scientific perspective, this decline does not merely signify a natural change in opinion, but rather a successful cognitive operation aimed at inducing cognitive fatigue [13] and the subsequent reactivation of latent neutrality narratives. This return to 2019 values demonstrates that the temporary "shock resilience" observed in 2022 lacked deep institutional anchoring [36]. In the absence of a robust value-based foundation, the Slovak cognitive space succumbed to long-term information activities that leveraged the sleeper effect [17]. In this process, adversarial narratives (initially dismissed during the peak of the 2022 crisis) gradually eroded public consensus as the immediate emotional threat subsided, allowing "alternative" geopolitical frameworks to re-emerge as legitimate public discourse. This failure to convert a reactive posture into a permanent strategic mindset highlights a critical vulnerability in the state's cognitive defence mechanisms [39].

## **5.2. Social Cohesion and Horizontal Mistrust as a Structural Vulnerability**

In the theoretical section, the social layer of the cognitive dimension is defined as the space where individual decisions are filtered through cultural and societal norms. However, the latest data from the DEKK Institute point to a critical disintegration of this layer in Slovakia [41].

General interpersonal trust reaches a level of only 21,3%, with up to 77% of the population exhibiting chronic vigilance toward their surroundings [41]. From a scientific perspective, this state of horizontal mistrust represents an “open door” for cognitive operations. A society afflicted by a deficit of mutual trust lacks the necessary social cohesion required to absorb cognitive shocks. The adversary exploits this deficit to deepen polarization, transforming the cognitive layer of the information environment into a fragmented battlefield lacking a unified interpretive framework of reality [15].

## **5.3. Mechanisms of Cognitive Dissonance and Ideological Anchoring**

In accordance with the theory of cognitive dissonance, the Slovak public resorts to defensive psychological mechanisms to reconcile traditional cultural sentiments (Pan-Slavism) with the reality of the current conflict [33].

This process is facilitated by low trust in political institutions (Parliament 25,8%, Government 30%) [41], which creates an authority vacuum. Conspiracy narratives thrive in this vacuum, serving to reduce dissonance. If a citizen distrusts official institutions, they become more susceptible to confirmation bias, actively seeking out alternative sources that confirm their pre-existing beliefs, even when they contradict established facts [28].

## **5.4. Paralysis of the Will to Defend: From Cognitive Effect to Physical Inaction**

One of the key objectives of cognitive warfare is to induce “cognitive paralysis” [15]. An empirical manifestation of this state in Slovakia is the low willingness to actively defend the homeland (only 13% of the population) [42].

While trust in the Armed Forces of the Slovak Republic (63,3%) [41] remains high, making them an important institutional anchor, disinformation campaigns (e.g., regarding the refusal of extraordinary service) specifically target this cognitive component. The successful exploitation of fear and information overload led to over 40,000 citizens taking administrative action to refuse service [42]. This case demonstrates how a cognitive operation moves from the virtual dimension (information on social media) through the cognitive dimension (interpretation of threat and fear) to the physical dimension (a legal act), thereby directly threatening the state’s strategic mobilization potential [31].

## **5.5. Synthesis of Findings: The Imperative of Cognitive Resilience**

The analysis confirms that the cognitive dimension of the Slovak Republic’s information environment is in a state of acute threat. Structural vulnerabilities (low social cohesion, institutional mistrust, and susceptibility to cognitive biases) enable an adversary to effectively manipulate the collective perception of reality.

Following the theoretical “whole-of-society approach”, it is evident that the solution cannot be exclusively technological. Since the Armed Forces of the Slovak Republic maintain a high credit of trust, they must play an active role in cognitive defence during peacetime. Transforming activities such as Preparation of the Population for State Defence [10] from technical training into tools for cognitive resilience (critical thinking training, recognition of psychological operations) is a prerequisite for ensuring the cognitive sovereignty of the population. Without restoring basic trust and resilience against psychological pressure, Slovak society remains vulnerable to operations whose goal is fragmentation and strategic paralysis of the state [9,26].

## **6. Conclusions**

The presented study confirms that the cognitive dimension of the information environment is no longer merely a theoretical concept but a real and critical battlefield of modern conflict. Through the analysis of NATO theoretical frameworks and their application to the current security context of the Slovak Republic, we have demonstrated how interactions within the virtual and physical dimensions generate direct effects on the minds and attitudes of the population.

Empirical data clearly indicate that the structural vulnerability of Slovak society (characterized primarily by chronic horizontal mistrust and a susceptibility to cognitive dissonance) enables adversarial actors to achieve strategic paralysis of the state without the use of kinetic force. The case of the mass refusal of extraordinary service illustrates a dangerous transition of a cognitive effect (fear and disinformation) into a physical act, which directly undermines the mobilization potential and defensive capability of the Slovak Republic.

Given that the Armed Forces of the Slovak Republic maintain a high level of public trust, they represent a key institutional pillar for building societal resilience. The primary conclusion of this work is that the process of Preparation of the Population for State Defence must adapt to the threats of the 21st century. It is no longer sufficient to focus exclusively on physical preparedness and technical skills. Modern state defence must integrate a cognitive component

that equips citizens with the mental tools to recognize psychological operations and resist manipulative narratives. Only through such a transformation can the Slovak Republic ensure its cognitive sovereignty and protect the integrity of its democratic decision-making processes.

**Acknowledgements.** The paper has been supported by the outputs of the research project "NI4200646 - Concept of the Slovak Armed Forces operations in the information domain" funded by the Ministry of Defence of the Slovak Republic through the inter-ministerial sub-program 06EOI-Research and development in support of state defence.

## References

1. Ivančík, R., Nečas, P. Air Transport Terrorism: One of the most Feared Types of Asymmetric Security Threat. INCAS Bulletin, 2020, Volume 12, Issue 4, pp. 227-239. <https://doi.org/10.13111/2066-8201.2020.12.4.21>
2. Ušiak, J., Ivančík, R. Economy and defence in the NATO member states. Economic Annals, 2014, Volume 7-8, Issue 2, pp. 8-11. <https://ea21journal.world/index.php/ea-v143-02/>
3. NBÚ. Krátky slovník hybridných hrozieb, (n. d.). [Online]. Available at: <https://www.nbu.gov.sk/kratky-slovník-hybridnych-hrozieb/>
4. AAP-06. NATO Glossary of Terms and Definitions (English and French). Brussels: NATO Standardization Office, 2021, 298 p.
5. Andrassy V., Ondruš M. The Gray Zone and Its Place in Security Environment. Brno: 4th International Conference CNDCGS, 2024. [Online]. Available at: View of Vol. 1 No. 1 (2024): CNDCGS'2024
6. Claveire, B. Cognitive warfare: the new battlefield exploiting our brains, 2025. [Online]. Available at: <https://www.polytechnique-insights.com/en/columns/geopolitics/cognitive-warfare-the-new-battlefield-exploiting-our-brains/>
7. Kolomazník T. Strategic Communication's Role in Eliminating Disinformation's Impact in Time of Current Geopolitical Challenges. Brno: 4th International Conference CNDCGS, 2024. [Online]. Available at: View of Vol. 1 No. 1 (2024): CNDCGS'2024
8. AJP-10.1. Allied Joint Doctrine for Information Operations. Brussels: NATO Standardization Office, 2023, 113 p.
9. MoD SR. Komunikačná stratégia rezortu obrany, 2021. [Online]. Available at: <https://www.mosr.sk/komunikacna-strategia-rezortu-obrany/>
10. MoD SR. Príprava obyvateľstva na obranu štátu (PONOS), 2021. [Online]. Available at: <https://www.mosr.sk/priprava-obyvatelstva-na-obranu-statu-ponos/>
11. AJP-10. Allied Joint Doctrine for Strategic Communications. Brussels: NATO Standardization Office, 2023, 117 p.
12. SPJ-A-10/StratCom. Strategická komunikácia. Bratislava: Generálny štáb OS SR, 2024, 107 p.
13. Sparling, R. Information overload. 2022. [Online]. Available at: <https://www.ebsco.com/research-starters/library-and-information-science/information-overload>
14. Claveire, B., du Cluzel, F. The Cognitive Warfare Concept, 2021. NATO Allied Command Transformation (ACT) Innovation Hub. [PDF]
15. Deppe, Ch., Schaal, G. S. Cognitive warfare: a conceptual analysis of the NATO ACT cognitive warfare exploratory concept, 2024. [Online]. Available at: <https://www.frontiersin.org/journals/big-data/articles/10.3389/fdata.2024.1452129/full>
16. Gisselsson Nord, D., Rinaldi, A. Cognitive warfare: why wars without bombs or bullets are a legal blind spot, 2025. [Online]. Available at: <https://theconversation.com/cognitive-warfare-why-wars-without-bombs-or-bullets-are-a-legal-blind-spot-260607>
17. Hovland, C. I., Weis, W. The Influence of Source Credibility on Communication Effectiveness in The Public Opinion Quarterly Volume 15, No. 4, 1951-1952, p. 635-650.
18. Levin, I. P., Schnittjer, S. K., Thee, S. L. Information framing effects in social and personal decisions in Journal of Experimental Social Psychology Volume 24, Issue 6, 1988, p. 520-529. [https://doi.org/10.1016/0022-1031\(88\)90050-9](https://doi.org/10.1016/0022-1031(88)90050-9).
19. Vráb V., Zezula J. The Role of Artificial Intelligence in Military. Brno: 4th International Conference CNDCGS, 2024. [Online]. Available on internet: View of Vol. 1 No. 1 (2024): CNDCGS'2024
20. Nissen, T. E. The Weaponization of Social Media. Characteristics of Contemporary Conflicts. Copenhagen: Danish Defence Collage, 2015, 150 p. ISBN: 978-87-7147-098-7.
21. AJP-01. Allied Joint Doctrine. Edition F, Version 1. Brussels: NATO Standardization Office, 2022, 166 p.
22. Ruhl. Ch. Cognitive Bias: How We Are Wired to Misjudge, 2023. [Online]. Available at: <https://www.simplypsychology.org/cognitive-bias.html>
23. SPJ-B-10-1/Oper. Informačné operácie. Bratislava: Generálny štáb OS SR, 2025, 99 p.
24. NATO Science and Technological Organization (STO). Cognitive Warfare. NATO Chief Scientist Research Report. Brussels: NATO STO-OCS, 2025, 24 p.

25. NATO StratCom COE. Kremlin Communication Strategy for Russian Audiences Before and After the Full-Scale Invasion of Ukraine. Riga: StratCom COE, 2023, 140 p. ISBN: 978-9934-619-47-2.
26. Zverec V. Hofstede's Cultural Model of Dimensions as an Analytical Tool for Comparison and Understanding Social Differences Between Nations. Liptovský Mikuláš: Vojenské Reflexie, 2024, 121 p.
27. Tversky, A., Kahneman, D. Availability: A heuristic for judging frequency and probability in Cognitive psychology, 1973, 5, p. 207-232.
28. Mc Raney, D. You Are Not So Smart. London: Penguin Group (USA), 2011, 127 p. ISBN: 978-1-101-54535-5.
29. Mintal, M. Dezinformácie a konšpiračné teórie v masmediálnom priestore in Vojenská osveta: spoločenskovedné semináre: 2021-2022/1. vydanie. Liptovský Mikuláš: PÚ OS SR, 2022, p. 72-85. ISBN: 978-8-089-60928-4.
30. Bezpečnostná stratégia SR, 2021. [Online]. Available at: <https://www.mosr.sk/bezpecnostna-strategia-sr/>
31. SIS. Správa o činnosti SIS za rok 2022, 2023. [Online]. Available at: <https://www.sis.gov.sk/pre-vas/sprava-o-cinnosti-2022.html>
32. Mesežnikov, G. Aké je to s ruskou propagandou v Európe (názor), 2019. [Online]. Available at: <https://www.aktuality.sk/clanok/525029/ake-je-to-s-ruskou-propagandou-v-europe-nazor/>
33. SAV. Vedec ÚPV SAV, V.V. I., sa podieľal na analýze fenoménu panslavizmu v súčasnosti, 2024. [Online]. Available at: [https://www.sav.sk/?lang=sk&doc=services-news&source\\_no=20&news\\_no=11665](https://www.sav.sk/?lang=sk&doc=services-news&source_no=20&news_no=11665)
34. Smoleňová, I. The Pro-Russian Disinformation Campaign in the Czech Republic and Slovakia. Types of media spreading pro-Russian propaganda, their characteristics and frequently used narratives. Prague: Prague Security Studies Institute, 2015. 18 p. [Online]. Available at: [https://www.hom-bre.cz/images/253\\_is-pro-russian-campaign.pdf](https://www.hom-bre.cz/images/253_is-pro-russian-campaign.pdf)
35. Hofstede, G. Dimensionalizing Cultures: The Hofstede Model in Context, 2011. [Online]. Available at: <https://scholarworks.gvsu.edu/orpc/vol2/iss1/8/>
36. Fábik, D. Prečo Slovensko podlieha ruskej propagande? 2023. [Online]. Available at: <https://dennikn.sk/3532347/preco-slovensko-podlieha-ruskej-propagande/>
37. Encyklopaedia Beliana. Kognitívna disonancia, 2017. [Online]. Available at: <https://beliana.sav.sk/heslo/kognitivna-disonancia>
38. Silenská, N. Expertka: Ruská ambasáda na Slovensku je najaktívnejší zastupiteľský úrad z celej Európy, 2024. [Online]. Available at: <https://euractiv.sk/section/digitalizacia/interview/ruska-ambasada-na-slovensku-najaktivnejši-zastupitelsky-uradom-eu-dezinformacie-propaganda/>
39. GLOBSEC. GLOBSEC Trends 2022 Slovakia. Bratislava: GLOBSEC, 2022, 9 p.
40. NATO. The Secretary General's Annual Report 2023. Brussels: NATO, 2024, 172 p.
41. DEKK Institute. Trendy (ne)dôvery 2025. Bratislava: DEKK Institute, 2025, 40 p.
42. Hutko, D. Klamstvá, strašenie aj reálne obavy. Slováci vo veľkom odopierajú vojenskú službu, 2023. [Online]. Available at: <https://spravy.pravda.sk/domace/clanok/657055-vyhlasenie-o-odopreti-vykonu-mimoriadnej-sluzby-podalo-vyse-40-tisic-obcanov/>

**Disclaimer/Publisher's Note:** The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of CNDCGS 2026 and/or the editor(s). CNDCGS 2026 and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.