

Studia Bezpieczeństwa Narodowego
Zeszyt 39 (2026)
ISSN 2028-2677, s. 101-120
DOI: 10.37055/sbn/226111

Instytut Bezpieczeństwa
Wydział Bezpieczeństwa, Logistyki i Zarządzania
Wojskowa Akademia Techniczna
w Warszawie

National Security Studies
Volume 39 (2026)
ISSN 2028-2677, pp. 101-120
DOI: 10.37055/sbn/226111

Institute of Security
Faculty of Security, Logistics and Management
Military University of Technology
in Warsaw

STATE SECURITY IN THE CONTEXT OF COGNITIVE WARFARE THREATS

BEZPIECZEŃSTWO PAŃSTWA W KONTEKŚCIE ZAGROZEŃ WOJNY KOGNITYWNEJ

Marcin MISZCZUK

ORCID: 0000-0001-5417-1903

Abstract. The aim of the article is to explain the nature of threats associated with cognitive warfare and to identify measures adopted by the state to counteract them. The main research problem is formulated as the following question: how to ensure state security in the face of threats arising from cognitive warfare? In order to address the primary research problem, it was analytically disaggregated into two subsidiary research questions. The first one is formulated as follows: what is the essence of the threats generated by cognitive warfare? The second addresses the following issue: what measures are to be implemented by the state to counteract the impact of cognitive warfare? The following main hypothesis has been adopted: it is assumed that if states implement proactive measures, including early detection of cyber threats, enhanced international cooperation in combating disinformation, the establishment of adaptive and effective legal frameworks, and the development of societal resilience to cognitive challenges, they will create the necessary conditions for effectively mitigating threats arising from cognitive warfare. The findings of the study indicate that threats associated with cognitive warfare constitute one of the principal challenges to contemporary state security, exerting a significant influence on the capacity of societies and armed forces to independently interpret information, accurately assess situational contexts, and undertake rational decision-making processes. The non-kinetic instruments employed within the framework of cognitive warfare enable deliberate interference in the cognitive processes of individuals and social groups, thereby facilitating the shaping of perceptions, attitudes, and behavioral patterns in accordance with the strategic objectives of the influencing actor. Consequently, the cognitive domain has emerged as a critical arena of strategic competition, the significance of which for the functioning and security of the state continues to increase in parallel with ongoing technological and informational developments. Accordingly, the effective mitigation of threats generated by cognitive warfare necessitates the development and reinforcement of state resilience across societal, institutional, and military dimensions. Such efforts should be grounded in the implementation of comprehensive and multidimensional measures encompassing the enhancement of citizens' information literacy and critical analytical competencies, the advancement of mechanisms for the identification, monitoring, and assessment of disinformation and psychological operations, as well as the integration of advanced information and communication technologies aimed

at strengthening cybersecurity. In this regard, building resilience within the cognitive domain should be regarded as an essential component of state security policy and a prerequisite for maintaining the nation's capacity to respond effectively to the evolving character of contemporary threats. The research methodology applied in this study comprises critical analysis and evaluation of the literature, systemic analysis, reasoning, synthesis and the prognostic method.

Abstrakt. Celem niniejszego artykułu jest eksplanacja istoty zagrożeń związanych z wojną kognitywną oraz identyfikacja działań państwa podejmowanych na rzecz przeciwdziałania im. Główny problem badawczy zawiera się w formie pytania: w czym wyraża się proces zapewniania bezpieczeństwa państwa w obliczu zagrożeń wynikających z wojny kognitywnej? W celu rozwiązania głównego problemu badawczego konieczna była jego fragmentacja na dwa problemy szczegółowe. Pierwszy z nich brzmi następująco: jaka jest istota zagrożeń generowanych przez wojnę kognitywną? Drugi problem badawczy wyraża się w formie następującego pytania: jakie działania podejmuje państwo na rzecz przeciwdziałania skutkom wojny kognitywnej? Przyjęto następującą hipotezę główną: przypuszcza się, że jeśli państwa podejmą działania o charakterze proaktywnym, obejmujące w szczególności wczesną detekcję zagrożeń w cyberprzestrzeni, intensyfikację współpracy międzynarodowej w zakresie przeciwdziałania dezinformacji, tworzenie adaptacyjnych i efektywnych ram prawnych oraz wzmacnianie odporności społecznej na wyzwania o charakterze poznawczym, wówczas będą w stanie stworzyć warunki niezbędne do skutecznego przeciwdziałania zagrożeniom wynikającym z wojny kognitywnej. W wyniku procesu badawczego ustalono, iż zagrożenia wynikające z wojny kognitywnej stanowią segment kluczowych wyzwań dla współczesnego bezpieczeństwa państwa, oddziałując przede wszystkim na zdolność społeczeństw oraz sił zbrojnych do autonomicznej interpretacji informacji, właściwej oceny sytuacji oraz podejmowania racjonalnych decyzji. Wykorzystywane w jej ramach instrumenty o charakterze niekinetycznym umożliwiają ingerencję w procesy poznawcze jednostek i grup społecznych, prowadząc do kształtowania percepcji, postaw oraz wzorców zachowań zgodnych z zamierzeniami podmiotu oddziałującego. Tym samym domena poznawcza staje się istotnym obszarem rywalizacji strategicznej, którego znaczenie dla funkcjonowania państwa systematycznie wzrasta. W konsekwencji skuteczne przeciwdziałanie zagrożeniom generowanym przez wojnę kognitywną wymaga budowy i wzmacniania odporności państwa na poziomie społecznym, instytucjonalnym oraz militarnym. Proces ten powinien opierać się na wdrażaniu wielowymiarowych rozwiązań obejmujących rozwój kompetencji informacyjnych obywateli, doskonalenie systemów identyfikacji i monitorowania operacji dezinformacyjnych oraz psychologicznych, a także wykorzystanie zaawansowanych technologii informacyjno-komunikacyjnych wpływających na cyberbezpieczeństwo. Metody badawcze wykorzystane w pracy to: krytyczna analiza i ocena literatury, analiza systemowa, wnioskowanie, synteza oraz prognozowanie.

Keywords: Cognitive warfare, non-kinetic operations, military security, North Atlantic Treaty Organization, threat development forecast.

Słowa kluczowe: Wojna kognitywna, działania niekinetyczne, bezpieczeństwo militarne, Sojusz Północnoatlantycki, prognoza rozwoju zagrożeń.

Introduction

The essence of state security resides in the capacity to counteract threats to its functioning and to foster conditions that support sustainable long-term development. The internal and external environments of the state continually generate challenges and threats to its security, which serve as an impetus for the state to undertake deliberate measures aimed at mitigating these threats within the broader framework of ensuring security. Security should not be understood solely as an end state to be achieved - rather, it constitutes an ongoing, continuous process. The processual nature of security is reflected in the systematic application by states of repeatable, purposefully designed methods and strategies in the pursuit of maintaining and

enhancing security (Pokruszyński, Piwowarski 2019, p. 79). The domains of homeland security, considered from the perspective of the state as the primary security actor, have evolved in response to civilizational and technological developments. These domains are not mutually exclusive; rather, they constitute an interconnected system in which each component influences the functioning of the others as well as the system as a whole. Among the domains of state security, the following can be distinguished: military, political, economic, social, environmental, cultural, informational, public security and cybersecurity (Gryz, Kitler 2014, pp. 24-25).

Contemporary means and methods of international competition extend far beyond the use of military force, often prioritizing alternative forms of influence that do not involve the kinetic employment of armed forces. Moving away from the overt use of military means beyond the threshold of open armed conflict allows for the blurring of responsibility, reduction of costs, and avoidance of the risk of a symmetrical response from the targeted actor. The transfer of warfare into the mental domain does not reduce threats; rather, it signifies their evolution, thereby providing a basis for state authorities and services to undertake proactive measures aimed at countering competition in the cognitive domain. The contemporary development of information technologies, leading to the networking of the world and globalization, the growing popularity of social media, and the migration of life into cyberspace, has transformed information into a strategic instrument of power, which has become a modern weapon, often employed without the awareness of the target. In contemporary military and strategic doctrine, five primary operational domains are formally recognized: land, maritime, air, space, and cyberspace. Alongside these, the cognitive domain emerges as an equally relevant component of the operational environment; however, it is still characterized by limited conceptual development, structural ambiguity, and significant uncertainty. Consequently, the preparation of strategies, directives, and courses of action in the event of a cognitive warfare threat is inherently a more demanding task (Szczygielska 2025, pp. 30-31).

The attainment of strategic advantage fundamentally depends on the proficient application of instruments of military and non-military power against an adversary through the deliberate generation of specific effects—be they physical, virtual, or cognitive. Despite technological transformations in the conduct of armed conflict and international competition, the conceptual foundation of contemporary understandings of war and state power remains rooted in the Clausewitz's *trinitarian model of war*. The Prussian military theorist identified three essential components of the state, the disruption or degradation of which would ultimately precipitate its defeat. In contemporary interpretations, this trinity is often represented by government, society, and the armed forces. The predominant role of information in the contemporary international security environment enables the disruption of the balance envisioned in the classical *war triad* framework. External actors possess both the capability and the intent to influence societies by shaping desires and preferences.

Influence operations that operate within the cognitive domain undermine target audiences, generating specific cognitive effects. Given the presence of free media, unrestricted access to the internet, and the protection of freedom of expression, democratic states are particularly susceptible to potent influence efforts by external actors aiming to secure strategic advantage within the cognitive sphere (Nieto 2024, pp. 1-4).

The international security environment appears to be approaching an era characterized by cognitive warfare, blurring the boundaries between peace and conflict. Human perceptions, beliefs, and decision-making processes can increasingly become targets of manipulation and exploitation. Shaping the minds and decisions of societies, policymakers, and military commanders has become—and is likely to remain—the essence of cognitive warfare. In the context of national and international security, it is evident that contemporary states and nations must be prepared to confront the challenges and threats posed by cognitive warfare—that is, a form of conflict whose symptoms remain largely imperceptible, and by the time its effects manifest, it is often far too late to respond effectively.

Current state of knowledge

The theory of cognitive warfare has been the subject of numerous studies. Among the most important works are those by the following authors: Bernard Claverie, Francois du Cluzel („The Cognitive Warfare Concept”), Agnieszka Szczygielska („Wojna kognitywna w ujęciu systemowym”, „Wojna kognitywna – źródła i zasadnicze cechy”), David Pappalardo („La guerre cognitive: agir sur le cerveau de l’adversaire”), Michael J. Cheatham („Wars of Cognition. How Clausewitz and Neuroscience Influence Future War-Fighter Readiness”) and David Ronfeldt, John Arquilla („Whose Story Wins”). These publications constitute a critical theoretical framework for the systematic investigation of threats emerging from cognitive warfare. They also provide a foundation for the practical application of this knowledge in the development and formulation of strategies aimed at mitigating, countering, and preemptively addressing such threats.

Despite the considerable number of publications concerning the operational use of cognitive warfare, authors such as: Marek Wrzosek („Wojny przyszłości. Doktryna, technika, operacje militarne”, „Działania psychologiczne w konfliktach nowego wieku”), Yamaguchi Shinji, Yatsuzuka Masaaki, Mommra Rira („China’s Quest for Control of the Cognitive Domain and Gray Zone Situations”), Amrita Jash („Fight and Win Without Waging a War: How China Fights Hybrid Warfare”), Yuriy Danyk, Chad M. Briggs („Modern Cognitive Operations and Hybrid Warfare”) and Tzu-Chieh Hung, Tzu-Wei Hung („How China’s Cognitive Warfare Works: A Frontline Perspective of Taiwan’s Anti-Disinformation Wars”), the existing knowledge

necessitates both supplementation and revision. In particular, the experiences of NATO's eastern flank states warrant close examination, as they provide critical insights for understanding regional security dynamics in the context of emerging cognitive warfare threats.

There are publications that partially address the issue of a state's defensive measures in response to cognitive warfare, as well as the strategies employed by collective security organizations to prevent and counter such threats, including works by: Robert Reczkowski, Andrzej Lis („Cognitive Warfare: what is our actual knowledge and how to build state resilience?”), Ignacio Nieto („Spanish Approach to Cognitive Warfare”), Christoph Deppe, Gary S. Schaal („Cognitive warfare: a conceptual analysis of the NATO ACT cognitive warfare exploratory concept”), Miina Kaarkoski („NATO's Concept of Cognitive Warfare”), Andrii Paziuk, Dmytro Lande, Elina Shnurko-Tabakova, Phillip Kingston („Decoding manipulative narratives in cognitive warfare: a case study of the Russia-Ukraine conflict”) and Beatrice Catena, Ondrej Ditrych, Nada Kovalcikova („Building EU resilience against manipulation through cognitive security”). Although the knowledge presented in these publications is methodologically sound and analytically robust, it requires further supplementation and systematic structuring. In particular, the material addressing a systemic approach to countering cognitive warfare should be organized in a coherent framework, with emphasis on the multi-vector strategies implemented by states, encompassing all structural components of the state apparatus, and further reinforced through cooperation within collective security organizations.

In light of the arguments presented, the issue of contemporary state security in relation to the spectrum of threats generated by cognitive warfare is both significant and cognitively relevant. The objectively existing gap in knowledge justifies undertaking research on this subject not only from a theoretical perspective but also as a necessary step toward the development of practical solutions. Issues related to cognitive warfare and operations in the noosphere permeate virtually every sphere of state activity and contemporary society. Consequently, there is a pressing need to intensify conceptual and doctrinal efforts aimed at developing solutions capable of countering these adverse phenomena and mitigating their effects. The pursuit and systematization of solutions aimed at building states' resilience against the challenges and threats posed by cognitive warfare also have a utilitarian dimension, directly contributing to the strengthening of a state's capacity for survival and development.

Research methodology

The conclusions drawn from the analysis of the available literature allow for the assertion that issues related to state security represent a subject of heightened academic interest due to the dynamic character of political processes and the evolving

challenges and threats. In view of the above, and based on the presented problem situation, the focus of this study was placed on the security of the state, examined in relation to the cognitive warfare threats. The aim of the research underlying this article was to explain the nature of threats associated with cognitive warfare and to identify measures adopted by the state to counteract them. On the basis of an objectively existing knowledge gap, the main research question was formulated as follows: how to ensure state security in the face of threats arising from cognitive warfare? This identified problem situation led to the formulation of the following specific research questions:

- what is the essence of the threats generated by cognitive warfare?
- what measures are to be implemented by the state to counteract the impact of cognitive warfare?

The following main hypothesis has been adopted: it is assumed that if states implement proactive measures, including early detection of cyber threats, enhanced international cooperation in combating disinformation, the establishment of adaptive and effective legal frameworks, and the development of societal resilience to cognitive challenges, they will create the necessary conditions for effectively mitigating threats arising from cognitive warfare.

The research process was structured in three principal stages. In the preliminary stage, the study was conceptualized. The existing gap in knowledge regarding the subject was identified, enabling the formulation of the research problem. During this stage, the primary research question and the overall objective of the study were defined, and the research methods, tools, and techniques to be applied in the main stage were selected. The main stage of the research involved addressing the primary and specific research questions through the systematic application of the selected methods, tools, and techniques. Finally, in the concluding stage, the findings of the research were synthesized, and overarching conclusions were drawn.

In the research process, a synchronization of diagnostic and prognostic approaches was undertaken. Among the methods employed, particular emphasis was placed on the critical analysis and evaluation of the literature, systemic analysis, reasoning, synthesis and the prognostic method. The use of critical analysis and evaluation of the literature allowed for the identification of the current state of knowledge in the available scholarly publications. This made it possible to define a cognitive gap within the field of study and, consequently, to determine the originality of the issues examined in the context of the existing literature. The application of systemic analysis enabled a comprehensive assessment of contemporary state security in light of the complexity of interrelations among various sectors and domains. Deductive

reasoning was employed with the aim of delineating the essence of threats posed by cognitive warfare and assessing their overarching impact on state functioning. Reductionist reasoning was utilized to facilitate the development of general recommendations for actions that should be undertaken by the state to foster resilience against the threats of cognitive warfare. Through the application of synthesis, the research problem was formulated, and the results of the study were summarized in the concluding section of the article. The prognostic method was used to formulate proposals for state-level measures to counter cognitive warfare and to project the future character of threats stemming from cognitive operations.

The essence of the threats generated by cognitive warfare

Contemporary scholarship conceptualizes the operational environment as comprising three fundamental, mutually interdependent dimensions: the physical, informational, and cognitive. The physical dimension refers to the material substrate of the environment, encompassing observable and persistent entities such as objects, resources, instruments, and other tangible means that constitute the infrastructural basis for action. The informational dimension is defined by the processes and systems governing the circulation of information, including the full lifecycle of data—its acquisition, collection, processing, filtering, storage, and dissemination—as well as the technological and organisational infrastructures enabling its transmission across networks and communication channels. By contrast, the cognitive dimension pertains to cognitive, neuropsychological, and psychosocial processes underlying human perception and decision-making. It includes the formation and evolution of motivational structures, belief systems, perceptual frameworks, and evaluative judgments, as well as value systems and affective states, including fear, uncertainty, and anxiety, all of which collectively shape individual and collective interpretation of reality. Owing to the extensive migration of private, professional, and interpersonal activities into the cyber domain, the volume, velocity, and intensity of information generation, storage, and exchange within digital ecosystems increasingly position cyberspace as a central infrastructural and functional nexus of contemporary socio-technical systems. In consequence, the spectrum of cognitive risks and vulnerabilities disseminated through cyberspace constitutes a salient and systemic threat to individuals, societies, and nation-states alike. The highly networked configuration of modern societies, coupled with the accelerated tempo of information circulation, enables the rapid, often near-instantaneous diffusion of harmful content, including manipulative communication strategies, propagandistic messaging, disinformation campaigns, and the amplification of extremist narratives (Jureńczyk, Baranowska, Wałdoch 2025, pp. 1-2).

Cognitive warfare represents an indirect form of coercion aimed at imposing the adversary's will. It is a non-kinetic mode of conflict that entails deliberate and systematic influence on targeted social groups, with the objective of undermining awareness, disrupting cognitive assessments, modifying patterns of thought, and consequently shaping behaviour. Cognitive warfare aims not only to influence and alter what society thinks, but, more importantly, to shape the very way of thinking. Cognitive operations involve influencing established mental patterns and modifying them by exploiting the inherent vulnerabilities of the human mind. They also exert influence over cognitive processes by filling existing knowledge gaps with one's own interpretations, narratives, or constructed realities. Consequently, actions in the cognitive domain are not merely intended to change perceptions; they also shape the cognitive process in a manner that favours the strategic objectives of the actor orchestrating the influence strategy (Claverie, du Cluzel 2022, pp. 2-3).

Cognitive warfare is inherently complex, involving an integrated use of informational, political, psychological, cyber, and social-engineering methods and instruments. A defining feature of cognitive warfare is the deliberate effort to deprive the targeted state of sovereignty and agency. External control over internal social and decision-making processes, combined with the weakening of core values and individual worldviews, results in the transformation of social attitudes and perceptions, objectives, systems of beliefs, and perspectives of social groups and entire nations. The propagation of false information, the amplification of polarizing narratives, the dissemination of fear and uncertainty, and the intensification of social antagonisms collectively contribute to a self-reinforcing spiral of societal destabilization. Cognitive operations are meticulously tailored to the target audience, leveraging beliefs, public sentiments, long-standing ethnic antagonisms, and contemporary social issues. This precise targeting renders them highly effective in altering mental maps and undermining willpower. Based on the practice of conducting cognitive operations, such activities are particularly associated with authoritarian and non-democratic states, which often employ extensive ideological and informational influence mechanisms targeting both their own citizens and armed forces (Danyk, Briggs 2023, pp. 35-38).

Cognitive operations can be conducted by a variety of actors, including states, substate organizations, armed forces, intelligence agencies, terrorist organizations, corporations, and radical religious groups. In terms of the targets of cognitive warfare, no society, nation, or individual can be considered immune to exposure to this form of aggression. The objective of cognitive-domain violence is to influence the cognition and behaviour of adversaries across three primary levels: societal, group, and individual. At the societal level, efforts are directed toward undermining the values underpinning democratic and social life, as well as the core ideas and objectives upheld by the nation. At the group level, cognitive operations aim to exacerbate

social polarization and erode trust in public institutions. At the individual level, such hostile actions—directed at civilians, personnel of the armed forces, and law enforcement institutions—seek to shape and recalibrate cognitive processes as well as decision-making capacities (Blatny 2025, p. 8).

Cognitive warfare may incorporate established non-kinetic influence methodologies, such as Information Operations (InfoOps), Psychological Operations (PsyOps), and Strategic Communication (StratCom). Nevertheless, both in theory and in practice, cognitive warfare extends well beyond the parameters of these conventional methods. Firstly, it is not constrained by specific techniques, methods, or means employed in campaigns, which may operate without a clearly defined or observable end state. Furthermore, cognitive warfare imposes no rigid criteria on the selection of target groups. Cognitive operations leverage the entire spectrum of contemporary communication tools to induce disruption and manipulate target audiences, functioning beneath the threshold of overt physical violence. A distinguishing feature of cognitive operations is their highly flexible scope and adaptable character. They may be conducted in conjunction with military operations, precede them, or be carried out independently of armed conflict. In cognitive warfare, narratives, methods, and objectives can be readily adapted to achieve the desired outcome, ranging from shaping the awareness of society and the adversary's armed forces regarding territorial conquests, influencing electoral processes, fostering antagonism among social groups, undermining military morale, encompassing both the degradation of communication channels and the extraction of sensitive data (Claverie, du Cluzel 2022, pp. 2-4). Cognitive operations are especially effective owing, in part, to their self-referential and recursive nature. Their effectiveness is reinforced by feedback mechanisms that continuously adapt influence activities to audience reaction (Szczygielska 2025, p. 513). Information operations and cognitive warfare are closely related but conceptually distinct. Information operations encompass activities designed to influence the information environment and shape the perceptions of target audiences through, among other means, disinformation, psychological operations, and strategic communication. Cognitive warfare, by contrast, represents a broader concept aimed at influencing human cognitive processes, including perception, beliefs, emotions, and decision-making. Consequently, information operations should be regarded as one of the instruments of cognitive warfare, whose primary domain of contestation is the human mind as a key arena of contemporary strategic competition (Wrzosek 2016, pp. 28-33).

The contemporary operational environment relies heavily on human cognitive capabilities; consequently, any error or weakness in the military decision-making process creates opportunities for the potential redirection of attention, perception, and cognitive processes to the adversary's advantage. Technological innovations, despite their wide range of benefits, are also exploited as entry points for external

influence operations, which manipulate human awareness and shape behaviour through communication tools. A core feature of war according to Clausewitz is its inherent unpredictability, driven by the deliberate actions of individuals within a volatile environment, where uncertainty in decision-making, often called the “fog of war”, plays a central role. In this context, the “fog” denotes a cognitive state induced by uncertainty and indecision, arising from the reception of specific environmental information, which impedes decision-making, delays cognitive processing, and constrains associative reasoning (Cheatham 2018, pp. 18-19). Nowadays, the term “mental fog” may also be applied to civilian environments. It is no longer the kinetic actions of an opponent, wartime propaganda messages, or influence agents (as in classical warfare) that generate impaired consciousness. In civilian contexts, particularly for adolescents and young adults (up to around 26 years of age), the primary factors contributing to mental fog include information overload, the dopamine-mediated reward mechanisms, exposure to trivial or empty content on social media, internal social polarization, and societal desensitization (Haywood, Rossell, Hart 2025, pp. 2-4). Inducing a state of “mental fog” within society mirrors the achievement of air superiority by air forces or the attainment of dominance in ground combat. It serves as the same prelude to a decisive strike. In cognitive warfare, a society deprived of focus, stripped of its own assessment of situations and social behaviours, incapable of making rational decisions, and lacking guiding values becomes a prepared battlefield for harmful cognitive operations (Blatny 2025, p. 6).

It should be emphasized that the initiation of cognitive operations is never arbitrary; rather, it is deliberately timed to coincide with circumstances, communications, or acts that produce a pronounced emotional or social effect on the target audience. Strategic examples of such opportune timing include attempts by hostile armed forces or unidentified actors to destabilize public order, migration pressures, protests, elections, natural disasters, and religious or national celebrations. The attainment of a cognitive window of superiority constitutes a critical determinant of success in the realm of cognitive competition. As articulated in *TRADOC Pamphlet 525-3-1, The U.S. Army in Multi-Domain Operations 2028*, a cognitive window of superiority is realized through the systematic degradation, disruption, and deliberate shaping of an adversary’s cognitive and decision-making processes. The achievement of such a state necessitates the calibrated and structured employment of influence upon the adversary’s societal structures—conceived as the internal environment of the organization—with the objective of generating conditions that are strategically advantageous. According to the doctrinal framework of the United States Armed Forces, the realization of a cognitive window of superiority necessitates the fulfillment of specific boundary conditions, predicated upon: a comprehensive understanding of the human factors inherent in the operational environment; the systematic integration of critical insights derived from the civilian

milieu into operational planning; and the deliberate shaping of societal perceptions to establish conditions conducive to the execution of military operations. This conceptual approach pertains to the conduct of military operations, in which human factors are construed as the cultural, psychological, and behavioral attributes of both individuals and collective groups. These human factors are referred to as factors capable of shifting attitudes and behaviour, insofar as they afford the capacity to modify previously stable and resistant attitudes, beliefs, and cognitive processes (TRADOC 2018, pp. 74-77).

Although definitively identifying all threats emanating from cognitive warfare presents inherent challenges, the unpredictability of its consequences nonetheless permits an attempt to systematically categorize the threats most frequently produced by this form of coercion. In order to delineate the spectrum of threats engendered by cognitive warfare, one may employ an illustrative analysis of cognitive operations as applied within the framework of the *Three Warfares* doctrine, which gives rise to threats associated with adverse influence on public opinion, psychological warfare, and legal warfare (Shinji, Masaaki, Rira 2023, pp. 40-41).

Threats associated with hostile influence on public opinion entail the deliberate construction and modulation of societal attitudes within a victim's populace, with the objective of creating conditions conducive to the attainment of political or military advantage. The victim may be subjected to the instrumentalization of informational resources and advanced technological capabilities to recalibrate the target society's perception of reality, erode collective morale, and enable the influencing actor to assert dominance over the strategic initiative. Such operations exert exogenous pressure on the orientation and evolution of social cognition within the victim state, resulting in a systematic reconfiguration of public opinion in a manner that privileges the influencing actor while generating adverse consequences for the targeted entity (Shinji, Masaaki, Rira 2023, pp. 40-41).

Cognitive warfare constitutes a multifaceted catalyst for profound socio-psychological disruption. Immediate deleterious effects manifest as the obfuscation of distinctions between reality and fiction, truth and falsehood; attenuation of collective volition and the capacity for autonomous decision-making; delegitimization of authority structures and historical veracity; and degradation of the integrative bonds linking the populace to the state. The protracted consequences encompass systemic indoctrination, uncritical assimilation of exogenous ideologies and behavioural norms, exacerbation of societal polarization, amplification of conflict-prone tendencies, proliferation of separatist movements, entrenched antagonism toward legitimate state authorities, and institutionalization of radical social dispositions. Prolonged engagement with cognitive operations engenders progressive normalization of behaviours and phenomena previously considered socially or morally unacceptable, culminating in their acceptance and eventual desirability - a process often described through the concept of the *Overton Window*. This normalization

process effectuates the decoupling of the populace from the strategic culture of the state, erosion of normative and moral constraints, and the strategic reconfiguration of collective religious, political, and ethnic identity (Szałek 2013, pp. 240-243).

A further category of cognitive threats may be identified in connection with the instrumentalization of legal warfare components. The essence of such threats resides in the strategic deployment of legal instruments as a means of securing asymmetrical advantage, facilitating the acquisition of political initiative, and ultimately enabling the attainment of military objectives. These manifestations include, *inter alia*, the deliberate induction of social unrest through the manipulation, selective framing, and amplification of information pertaining to the imposition of legal and trade sanctions upon a given state. The imposition of juridical pressure upon the victim is manifested through the normative preconditioning of prospective offensive actions by the aggressor. This, in turn, fosters a perception of the futility of resistance to armed aggression. Additionally, it involves the dissemination of selectively modified or reinterpreted legal acts. These are intended to engineer an adverse legal and political environment within a state subjected to cognitive warfare (Shinji, Masaaki, Rira 2023, pp. 41-42).

The threats engendered by cognitive warfare constitute a salient and increasingly complex challenge to the internal security architecture of contemporary democratic states. The accelerated advancement of information and communication technologies, the progressive networking of societies, and the partial migration of social, political, and economic life into virtual environments have collectively enabled adversarial actors to penetrate the informational space at the level of individual citizens through digitally mediated channels. Within this context, highly profiled and audience-tailored content functions as a primary vector for inducing cognitive and perceptual shifts, thereby facilitating susceptibility to manipulation and strategic influence. Accordingly, it is imperative to recognize the broad and multidimensional spectrum of risks that cognitive warfare poses to internal security. Among the most consequential manifestations is the potential for external interference in democratic electoral processes, accompanied by sustained, coordinated, and often covert influence operations targeting electorates. Such campaigns contributed to measurable shifts in voter preferences, particularly among undecided segments of the electorate, toward candidates espousing more radical or non-mainstream positions (Rickli, Knappe 2025, pp. 1-2).

A further salient example underscoring the susceptibility of contemporary states to cognitive warfare is provided by the global COVID-19 pandemic. Notwithstanding the fact that the majority of democratic governments enacted multifaceted response strategies—encompassing the introduction of emergency legislation, the declaration of states of emergency, the reinforcement of public healthcare systems, and the strategic reallocation of state resources. The informational environment and the cognitive domain of society emerged as particularly vulnerable

vectors of contestation. In this context, the pandemic could be conceptualized as a paradigmatic instance of a cognitively contested battlespace, shaped by the deliberate introduction of managed informational disorder by hostile state and non-state actors. Such operations were predicated upon the systematic delegitimization of epistemic authorities, particularly within the scientific and medical communities, and the large-scale dissemination of conspiratorial narratives. Disinformation thereby assumed the function of a strategic instrument designed not only to erode institutional trust, but also to recalibrate the epistemic frameworks through which individuals interpret risk, authority, and collective responsibility. Within the European context, these dynamics facilitated the consolidation of entrenched socio-political cleavages, most notably manifested in the dichotomization of public discourse into “pro-” versus “anti-vaccination” constituencies. Importantly, this division extended beyond the immediate question of public health, evolving into a broader normative conflict frequently framed in terms of “liberty” versus “security.” The resultant polarization was not merely discursive, but structurally embedded, contributing to the fragmentation of the public sphere. Consequently, the deployment of cognitive warfare mechanisms during a period already characterized by elevated systemic stress significantly intensified affective responses within societies, amplifying collective anxiety, fostering attitudinal radicalization, and exacerbating intra-societal divisions. In this sense, the pandemic functioned as both a catalyst and a force multiplier for cognitive vulnerabilities, revealing the extent to which crises can be instrumentalized to destabilize democratic cohesion from within (EEAS 2021).

Measures to be implemented by the state to counteract the impact of cognitive warfare

Considering that the threats associated with cognitive warfare are multidimensional and cross-cutting, encompassing the political, societal, and cognitive domains, the development of defensive capabilities against such threats must be conceived in a comprehensive and integrated framework. Drawing upon contemporary interpretations of Clausewitz’s *trinitarian model*, one may endeavour to formulate strategic recommendations and initiatives that, within the context of a contemporary democratic state, serve to reinforce: governance structures, societal resilience, and the operational capacity of the armed forces in countering the multifaceted challenges posed by cognitive warfare.

Ensuring the resilience of state institutions in the face of the multifaceted threats posed by cognitive warfare constitutes a highly complex undertaking, owing to the dynamic character of political processes, the persistent pressures exerted by adversarial external actors, and the proliferation of channels for the dissemination of influence operations. It is proposed that, at the central level, the enhancement

of state capacity should commence with the development of a strategic framework which may be encompassed within a document such as the proposed National Cognitive Security Strategy. The fundamental objective of this document would be to safeguard state institutions, citizens, security services, and critical infrastructure against the effects of cognitive warfare threats. Conceptually, the document could encompass several core components, including: a precise definition and typology of threats; the articulation of national objectives in the domain of counter-cognitive security; risk assessment and identification of principal security challenges; delineation of institutional protective measures and mechanisms; and a dedicated section addressing communication strategies and public awareness. It is evident that such a strategy would not operate in isolation, but would be embedded within Allied resilience and cognitive security frameworks, including those of NATO and the European Union. Alternatively, a dedicated section addressing cognitive security could be integrated into the overarching National Security Strategy. Irrespective of whether cognitive security is treated as the focus of an independent strategy or as a distinct chapter within a broader framework, it remains essential to formulate detailed ministerial-level operational plans that clearly delineate the responsibilities, roles, and objectives of the various state apparatuses in the identification, mitigation, and management of cognitive threats (Reczkowski 2026).

An additional mechanism for bolstering the resilience of national authorities against cognitive threats lies in the proactive identification of emergent threats potentially engineered by adversaries within the cognitive domain. A foundational and operationally parsimonious framework for countering cognitive influence can be conceptualised as comprising three sequential phases: detection, prevention, and mitigation. Within this architecture, advanced analytical instruments—such as “Attack Index”—alongside artificial intelligence-driven algorithms, are predominantly utilised in the detection phase. Attack Index is “*an integrated media threat indicator that takes into account such factors as general media activity, competitors’ activities, average background deviations, media attacks in progress and their stages, the history and development of a negative tone in publications, and the degree of information processes randomness*”(Attack Index 2026). These platforms facilitate the real-time monitoring of adversarial narratives, thereby enabling timely and calibrated responses to disinformation campaigns. They draw upon open-source data, artificial intelligence methodologies, and a suite of proprietary algorithms. The platforms also incorporate functionalities for systematic data collection and advanced data visualization. Furthermore, detection systems grounded in artificial intelligence are capable of identifying linguistic patterns and anomalies that may signal manipulative intent. AI-based models enable large-scale semantic analysis of extensive datasets, as they are capable of identifying not only overtly false statements but also more subtle forms of linguistic manipulation. Pre-trained models and Natural Language Processing (NLP) algorithms can detect phenomena such

as sarcasm, euphemistic language, and propagandistic framing. This facilitates the monitoring of emergent trends within the information environment, which may indicate an increasing exploitation by adversarial actors of cognitive biases as well as deeply entrenched socio-cultural stereotypes. Their primary function is the identification of emergent micro-trends, thematic clusters, and topics characterised by a high capacity to mobilise and amplify affective responses within public discourse. The early detection of such phenomena facilitates the timely recognition of external cognitive interference, thereby enabling the implementation of pre-emptive measures. At this juncture, a key intervention consists in the deployment of strategic communication activities. These are designed to systematically expose discrepancies between propagandistic content and empirically verifiable information, to elucidate the probable strategic objectives underlying adversarial information activities, and to strengthen the perceived legitimacy of state institutions and law enforcement agencies (Paziuk, Lande, Shnurko-Tabakova, Kingston 2025, p. 7).

Achieving such anticipatory insight requires medium- and long-term analyses of prospective narrative trajectories that may be leveraged as instruments of manipulation and influence over societal perceptions. The efficacy of defensive strategies fundamentally depends on the capacity to forecast which information vectors are likely to be propagated and to identify the critical junctures at which cognitive influence may be exerted. Put differently, the purpose of such analytical efforts should be conceptualized as twofold. First, they should aim to identify the anticipated intended outcomes of hostile activities conducted by state actors engaged in cognitive warfare. Second, they should facilitate the effective implementation of strategic communication processes designed to disseminate coordinated, nationwide awareness campaigns concerning issues with the potential to evolve into catalysts of societal tension or systemic instability. Such anticipatory intelligence materially enhances the ability of state actors to implement timely and targeted informational interventions within their own societies and to undertake corrective measures designed to invalidate or mitigate the impact of misleading or deceptive narratives (Bornio 2025). Given the inherently transboundary and partially deterritorialized nature of cyberspace, there is a corresponding need to further intensify and institutionalise international cooperation in the domain of cognitive security. In this context, key cooperative mechanisms may include the establishment of transnational fact-checking infrastructures, the formation of multinational analytical and intelligence-sharing teams, as well as sustained collaborative engagement within specialised working groups tasked with the development and refinement of doctrinal and strategic frameworks within multilateral organisations such as the European Union and NATO (Paziuk, Lande, Shnurko-Tabakova, Kingston 2025, pp. 11-13).

The enhancement of societal resilience to cognitive warfare should be conceptualized as a multidimensional and integrated approach, combining awareness-raising initiatives, educational frameworks, as well as legal and regulatory instruments. At the

outset, it is imperative to elevate public cognizance of the scale and gravity of cognitive threats, thereby fostering a baseline level of societal preparedness. This objective may be effectively pursued through the systematic incorporation of foundational knowledge into public information campaigns, state-supported digital platforms (including widely utilized citizen-oriented mobile applications), and mainstream broadcast media. Informed by the experience of the Swedish Government, particular attention should be devoted to the development and dissemination of universally accessible educational materials, formulated in clear and non-specialist language, aimed at introducing citizens across all demographic groups to the dynamics of the cognitive domain (*“Don’t be fooled – Handbook”, “Psychological defence and information influence – a textbook on theory and practice” and “Countering information influence activities”*) (Psychological Defence Agency 2026). Such instruments may serve as a foundational layer of societal immunization against manipulative informational influences. Furthermore, the role of high-quality general education remains indispensable in reinforcing the cognitive dimension of societal resilience. Crucially, this should not be narrowly construed as specialized training in counter-disinformation techniques, but rather as the systematic cultivation of critical thinking, intellectual autonomy, and analytical reasoning capacities. In this sense, education functions as a long-term structural determinant of societal robustness against cognitive manipulation. The core of counter-cognitive education should lie in structured training in media literacy. Such training ought to target social groups that are particularly vulnerable to disinformation, including young people and populations affected by digital exclusion, who are disproportionately exposed to hostile information influence. Finally, policy and regulatory mechanisms constitute an essential pillar underpinning societal resilience. These should encompass, *inter alia*, the protection of intellectual property rights and the safeguarding of individual privacy, both of which are increasingly implicated in the dynamics of information manipulation. Concurrently, the deployment of advanced technological solutions plays a critical role in mitigating the weaponization of information, thereby contributing to the integrity and security of the broader information environment (Rickli, Knappe 2025, p. 2).

Within the domain of reinforcing the cognitive resilience of the armed forces against hostile cognitive operations, three fundamental support mechanisms may be analytically distinguished. First, the systematic and sustained defensive actions aimed at degradation of an adversary’s capacity to design, coordinate, and execute influence operations. Second, the comprehensive enhancement of cognitive awareness at both the individual level—encompassing the perceptual, psychological, and behavioural preparedness of military personnel—and the technological level, understood as the situational and informational awareness of subunits and tactical formations operating within a complex, information-saturated environment. Third, the development and institutionalization of advanced capabilities to counter and

neutralize cognitive campaigns, ensure the rapid reconstitution and sustainment of operational effectiveness under conditions of persistent cognitive pressure, and safeguard the continuity, coherence, and procedural integrity of the Military Decision-Making Process (Cleveland, Brookes, Maxwell 2026).

NATO is adopting a long-term, proactive approach to cognitive warfare, integrating cognitive considerations into multi-domain operations and embedding the cognitive domain within its strategic culture and operational doctrine. This includes the incorporation of cognitive factors into defence planning and capability development cycles, the application of simulation environments and experimental exercises to evaluate cognitive threat scenarios, and the formulation of strategic recommendations regarding the responsible use of emerging technologies, particularly artificial intelligence. Through these initiatives, NATO aims to maintain strategic agility and operational effectiveness in an increasingly contested informational landscape, thereby safeguarding its decision-making autonomy and strengthening the collective security of its member states (Deppe, Schaal 2024, pp. 3-11).

Conclusions

The findings of this study support the argument that cognitive warfare is increasingly conceptualised as a distinct category within the contemporary spectrum of conflict, while simultaneously intersecting both conceptually and operationally with the traditional domains of land, maritime, air, and cyberspace operations. The primary significance of cognitive warfare lies in its capacity to exert pervasive and deleterious effects on individuals, social groups, and entire populations, with the objective of reshaping cognitive frameworks, influencing patterns of thought, and ultimately imposing the adversary's intended will. Its non-kinetic, subthreshold character constitutes a fundamental and persistent challenge for modern states and societies. Mitigating cognitive operations in real time poses particular difficulties, as the identification and attribution of hostile activities executed by specialized actors or military forces within the cognitive domain are inherently problematic. The lack of reliable attribution substantially diminishes the feasibility of implementing proportionate or equivalent responses. Consequently, it is widely acknowledged that the principal measures undertaken by contemporary democratic states to counteract cognitive warfare must be preemptive, focusing on anticipatory actions designed to reduce vulnerability prior to the manifestation of attacks. Prevention, therefore, emerges as a central principle of defense against cognitive threats. By contrast, the detection of operational effects typically signals that the state has already been targeted, at which juncture opportunities for effective mitigation are severely constrained, underscoring the critical importance of proactive resilience and strategic foresight.

The analysis suggests that the foundational premise for developing the state's comprehensive capacity to counter threats associated with cognitive warfare lies in the systematic identification of operational requirements across three core domains: governance structures, societal resilience, and the operational capacity of the armed forces. The subsequent phase entails the delineation and structuring of capability development trajectories within the aforementioned spheres of state functioning, in accordance with an integrated and system-oriented approach. Resilience to cognitive threats may be conceptualised as a systemic chain, the overall robustness of which is ultimately conditioned by its weakest link. From this perspective, ensuring adequate levels of resilience necessitates the implementation of coordinated, interagency, and multidimensional measures. Such measures are required, first, to enable the optimisation and harmonisation of operational capabilities across relevant domains, and second, to facilitate sustained inter-organisational cooperation in the context of countering cognitive warfare. A key insight emerging from this analysis is that effective societal defense against cognitive operations cannot be achieved solely through technological superiority or cyber defense measures. Beyond these capabilities, the efficacy of such defensive efforts is fundamentally conditioned by the level of public trust in legitimate authorities and the degree of civic literacy within the population. Societies characterized by strong civic cohesion and shared democratic values demonstrate markedly greater resilience against mechanisms intended to manipulate attitudes, beliefs, and decision-making processes.

BIBLIOGRAPHY

1. Allied Command Transformation, 2021. The NATO Warfighting Capstone Concept [online]. Available at: <https://www.act.nato.int/wp-content/uploads/2023/06/NWCC-Glossy-18-MAY.pdf>, [accessed: 10 April 2026].
2. Attack Index, 2026. User Manual [online]. Available at: <https://attackindex.com/en/user-manual/>, [accessed: 12 May 2026].
3. Blatny, J., 2025. Cognitive Warfare, Bruksela: NATO Science & Technological Organization.
4. Bornio, J., 2025. Działania kognitywne Rosji wobec Polski przy użyciu migrantów z obszaru postradzieckiego [online]. Available at: <https://ies.lublin.pl/komentarze/dzialania-kognitywne-rosji-wobec-polski-przy-uzyciu-migrantow-z-obszaru-postradzieckiego/#:~:text=%5B1%5D%20Dzia%C5%82ania%20kognitywne%20to%20aktywno%C5%9Bci,wobec%20jedynie%20okre%C5%9Blonej%20jego%20grupy>, [accessed: 17 March 2026].
5. Cheatham, M.J., 2018. Wars of cognition. How Clausewitz and neuroscience influence future war-fighter readiness. *Air & Space Power Journal* nr 32 [online]. Available at: https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-32_Issue-4/F-Cheatham.pdf [accessed: 11 March 2026].

6. Claverie, B., du Cluzel, F., 2022. The Cognitive Warfare Concept [online]. Available at: https://innovationhub-act.org/wp-content/uploads/2023/12/CW-article-Claverie-du-Cluzel-final_0.pdf, [accessed: 11 March 2026].
7. Cleveland, Ch.T., Brookes, D., Maxwell, D.S., 2026. Cognitive Warfare: An Allied Blueprint and a Pentagon Opportunity [online]. Available at: <https://smallwarsjournal.com/2026/01/16/cognitive-warfare/>, [accessed: 18 March 2026].
8. Danyk, Y., Briggs, Ch. M., 2023. Modern Cognitive Operations and Hybrid Warfare. *Journal of Strategic Security* 16 [online]. Available at: <https://digitalcommons.usf.edu/jss/vol16/iss1/3/> [accessed: 20.03.2026].
9. Deppe, Ch., Schaal, G.S., 2024. Cognitive warfare: a conceptual analysis of the NATO ACT cognitive warfare exploratory concept. *Frontiers in Big Data* nr 7 [online]. Available at: <https://www.frontiersin.org/journals/big-data/articles/10.3389/fdata.2024.1452129/full>, [accessed: 31 March 2026].
10. European External Action Service, 2021. EEAS special report update: Short assessment of narratives and disinformation around the COVID-19 pandemic [online]. Available at: <https://euvsdisinfo.eu/eeas-special-report-update-short-assessment-of-narratives-and-disinformation-around-the-covid-19-pandemic-update-december-2020-april-2021/> [accessed: 31 March 2026].
11. Gryz, J., Kitler, W., 2014. Identyfikacja, klasyfikacja, podział bezpieczeństwa państwa (narodowego), Warszawa: Akademia Obrony Narodowej.
12. Haywood, D., Rossell, S.L., Hart, N.H., 2025. Cutting through the fog: recognising brain fog as a significant public health concern. *BMC Public Health* 1 [online]. Available at: [12889_2025_Article_22525.pdf](https://www.bmcpublichealth.com/content/25/1/12889) [accessed: 11 March 2026].
13. Jureńczyk, Ł., Baranowska, A., Wałdoch, M., 2025. Instrumentalization of Pope Francis's Anti-War Discourse in the Cognitive Warfare of the Russian Federation. *Pastoral Psychology* [online]. Available at: <https://link.springer.com/article/10.1007/s11089-025-01252-0#citeas> [accessed: 21 April 2026].
14. Nieto, I., 2024. Spanish Approach to Cognitive Warfare [online]. Available at: <https://publications.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-HFM-361/MP-HFM-361-KN1.pdf> [accessed: 10 March 2026].
15. Paziuk, A., Lande, D., Shnurko-Tabakova, E., Kingston, P., 2025. Decoding manipulative narratives in cognitive warfare: a case study of the Russia-Ukraine conflict. *Frontiers in Artificial Intelligence* 8 [online]. Available at: <https://www.frontiersin.org/journals/artificial-intelligence/articles/10.3389/frai.2025.1566022/full>, [accessed: 21 April 2026].
16. Pokruszyński, W., Piwowarski, J., 2019. Bezpieczeństwo. Teoria i praktyka, Kraków: Naukowo-Wydawniczy Instytut Badań Bezpieczeństwa i Obronności WSBPI „Apeiron”.
17. Psychological Defence Agency, 2026. Handbooks [online]. Available at: <https://mpf.se/psychological-defence-agency/knowledge-and-support/handbooks>, [accessed: 10 May 2026].
18. Reczkowski, R., 2026. Wojny o serca i umysły [online]. Available at: <https://aktualnosci.aksim.edu.pl/publikacje/nauka/wojny-o-serca-i-umysly-3/#:~:text=Budowanie%20>

- odporno%C5%9Bci%20kognitywnej%20musi%20by%C4%87%20zadaniem%20systemowym., tworzy%C4%87%20jasne%20strategie%20przeciwdzia%C5%82ania%20dezinformacji%20i%20wojnie, [accessed: 17 March 2026].
19. Rickli, J-M., Knappe, T., 2025. Enhancing Cognitive Security and Societal Resilience to Counter Cognitive Warfare [online]. Available at: <https://www.gcsp.ch/publications/enhancing-cognitive-security-and-societal-resilience-counter-cognitive-warfare>, [accessed: 17 March 2026].
 20. Shinji, Y., Masaaki, Y., Rira, M., 2023. China's Quest for Control of the Cognitive Domain and Gray Zone Situations, Tokio: The National Institute for Defense Studies [online]. Available at: https://www.nids.mod.go.jp/publication/chinareport/pdf/china_report_EN_web_2023_A01_revised.pdf, [accessed: 10 April 2026].
 21. Szałek, B., 2013. Some Praxiological Reflections on the So-Called 'Overton Window of Political Possibilities,' 'Framing' and Related Problems. *Reality of Politics* nr 4 [online]. Available at: http://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.ojs-doi-10_15804_rop201315, [accessed: 11 March 2026].
 22. Szczygielska, A., 2025. Wojna kognitywna – źródła i zasadnicze cechy. *Kwartalnik Bellona* 1 [online]. Available at: <https://kwartalnikbellona.com/article/551652/pl>, [accessed: 09 March 2026].
 23. TRADOC, 2018. From Multi-Domain Battle to Multi-Domain Operations. TRADOC Pamphlet 525-3-1, The U.S. Army in Multi-Domain Operations 2028, Fort Eustis: United States Army Training and Doctrine Command [online]. Available at: <https://api.army.mil/e2/c/downloads/2021/02/26/b45372c1/20181206-tp525-3-1-the-us-army-in-mdo-2028-final.pdf>, [accessed: 02 March 2026].
 24. Wrzosek, M., 2016. Działania psychologiczne w konfliktach nowego wieku. *Kwartalnik Bellona* 2 [online]. Available at: <https://kwartalnikbellona.com/article/01.3001.0010.7327/pl>, [accessed: 09 April 2026].