УДК 327.8:355.“2022/2025”
DOI: https://doi.org/10.31652/2411-2143-2026-57-192-201

Cognitive counteraction by the West to Russian information influence: mechanisms, policies, and instruments (2022–2025)

Vadym Yu. Bespeka
Hetman Petro Sahaidachnyi National Army Academy of Ministry of Defense of Ukraine
PhD in History, Doctoral Student (Ukraine)
email: bvu1927@gmail.com
ORCID: https://orcid.org/0000-0002-3811-341X
Web of Sciense ResearcherID:https://www.webofscience.com/wos/author/record/GPS-8457-2022

Abstract.

The purpose *of the article is to provide an integrated analysis of the strategic approaches, instruments, and institutional arrangements of cognitive countermeasures employed by Western states and international organizations to neutralize Russian information influence during 2022–2025. The study covers the diplomatic, information-analytical, technological, and societal dimensions of the West's response to Russian influence operations.* ***The methodological framework*** *is based on structural-functional, comparative political, and information-analytical approaches, as well as content analysis of official documents, reports, digital platform data, and studies produced by NATO, the European Union, the G7, the Hybrid CoE, and independent research institutions. The article examines the evolution of strategic communications, the practice of pre-emptive intelligence declassification, the development of the OSINT ecosystem and fact-checking, sanctions-based public diplomacy, and technical tools for detecting and countering disinformation. Special attention is given to emerging threats associated with the use of generative AI in FIMI operations and to the responses of Western institutions to these challenges.* ***The scientific novelty*** *of the study lies in its integrated examination of Western cognitive countermeasures as a layered system encompassing diplomacy, digital security, algorithmic monitoring, artificial intelligence, fact-checking, and civic mobilization.* ***Conclusions.*** *During 2022–2025, Western approaches to cognitive countermeasures became substantially institutionalized and developed into a core element of security policy. A transition occurred from fragmented responses to a broad model integrating intelligence declassification, rapid debunking of hostile narratives, sanctions-based pressure, regulation of digital platforms, and the development of common strategic communication standards. Coordinated efforts by governments, supranational institutions, private companies, and civil society created a multi-layered deterrence ecosystem that significantly limited the effectiveness of Russian FIMI operations across the transatlantic space and in Ukraine. OSINT communities, automated manipulation detection tools, increasing media literacy, and the establishment of specialized centres for countering hybrid threats played an important role in this process. However, the current framework of countermeasures remains incomplete and still needs further refinement. The spread of generative AI, the emergence of high-quality deepfakes, circumvention mechanisms within the information ecosystems of the Global South, and the persistence of vulnerable audiences within Western societies create new challenges. Russian influence operations continue to adapt by combining social, political, and technological instruments while seeking to exploit internal crises within democratic states. Under these conditions, Western institutions require anticipatory planning, stronger regulatory frameworks, the integration of AI into protection and monitoring systems, and enhanced societal resilience through education, strategic communication, and cross-sectoral cooperation. Cognitive countermeasures are becoming a long-term, multidimensional, and technologically sophisticated component of contemporary security policy that requires the continuous refinement of approaches.*

Keywords: *cognitive operations, cognitive countermeasures, cognitive warfare, strategic communications, information resilience, FIMI, NATO, European Union.*

Когнітивна протидія Заходу російським інформаційним впливам: механізми, політики та інструменти (2022–2025)

Вадим Беспека
Національна академія сухопутних військ імені гетьмана Петра Сагайдачного
доктор філософії в галузі історії та археології, докторант
email: bvu1927@gmail.com
ORCID: https://orcid.org/0000-0002-3811-341X
Web of Sciense ResearcherID: https://www.webofscience.com/wos/author/record/GPS-8457-2022

Анотація.

Мета статті *– комплексно проаналізувати стратегічні підходи, інструменти та інституційні механізми когнітивної протидії, які західні держави та міжнародні організації застосовували для нейтралізації російських інформаційних впливів у 2022–2025 роках. Дослідження охоплює дипломатичний, інформаційно-аналітичний, технологічний і суспільний рівні реагування Заходу на російські операції впливу.* ***Методологічну*** *основу дослідження становлять структурно-функціональний, порівняльно-політологічний та інформаційно-аналітичний підходи, а також контент-аналіз офіційних документів, звітів, даних цифрових платформ, досліджень NATO, ЄС, G7, Hybrid CoE та аналітики незалежних дослідницьких інституцій. Проаналізовано еволюцію стратегічних комунікацій, практику превентивного розсекречення розвідданих, формування OSINT-екосистеми та фактчекінгу, санкційну публічну дипломатію, технічні інструменти виявлення та блокування дезінформації. Особлива увага приділена появі нових загроз, пов'язаних із використанням генеративного ШІ у FIMI-операціях, та реакції західних інституцій на ці виклики.* ***Наукова новизна*** *полягає у комплексному розгляді західної когнітивної протидії як багаторівневої системи, що охоплює дипломатію, цифрову безпеку, алгоритмічний моніторинг, штучний інтелект, фактчекінг і громадянську мобілізацію.* ***Висновки.*** *У 2022–2025 рр. західні підходи до когнітивної протидії суттєво інституціоналізувалися та перетворилися на стратегічний компонент політики безпеки. Відбувся перехід від фрагментарних реакцій до системної моделі, яка поєднує розсекречення розвідданих, оперативне спростування наративів противника, санкційний тиск, регуляцію цифрових платформ та формування спільних стандартів стратегічних комунікацій. Скоординовані дії урядів, наднаціональних структур, приватних компаній і громадянського суспільства створили багаторівневу екосистему стримування, що істотно знизила впливовість російських FIMI-операцій у трансатлантичному просторі та в Україні. Важливу роль відіграли OSINT-спільноти, автоматизовані інструменти виявлення маніпуляцій, зростання медіаграмотності населення й розвиток спеціалізованих центрів протидії гібридним загрозам. Водночас система протидії залишається незавершеною та потребує подальшого розвитку. Поширення генеративного ШІ, поява високоякісних діпфейків, обхідні механізми в інформаційних екосистемах Глобального Півдня і збереження вразливих аудиторій у самих країнах Заходу створюють нові виклики. Російські операції впливу продовжують адаптуватися, поєднуючи соціальні, політичні та технологічні інструменти й намагаючись експлуатувати внутрішні кризи демократичних держав. За цих умов західним інституціям потрібне випереджувальне планування, посилення регуляторної бази, інтеграція ШІ для захисту й моніторингу, а також зміцнення стійкості суспільств, зокрема через освіту, комунікацію та міжсекторальну взаємодію. Когнітивна протидія перетворюється на довгостроковий, багатовимірний і технологічно складний компонент сучасної політики безпеки, що потребує постійного вдосконалення підходів.*

Ключові слова: *когнітивні операції, когнітивна протидія, когнітивна війна, стратегічні комунікації, інформаційна стійкість, FIMI, НАТО, Європейський Союз.*

Problem Statement. During the full-scale aggression of the Russian Federation against Ukraine, the cognitive dimension of the confrontation intensified dramatically, with disinformation, manipulative narratives, psychological influence, and technologically sophisticated Foreign Information Manipulation and Interference (FIMI) operations becoming key instruments of Russia's hybrid strategy. In response, the United States, the European Union, the United Kingdom, NATO, and their partner institutions developed an integrated framework of cognitive countermeasures combining diplomatic, informational, legal, and technological mechanisms. Despite certain political differences among these actors, coordination of joint efforts in countering Russian information and cognitive operations was maintained. However, the scale of these influence operations, the nature of their institutionalization, the level of cross-sectoral integration, and their actual effectiveness under conditions of the rapid

evolution of digital threats remain insufficiently explored. This necessitates a systematic analysis of the strategic mechanisms and technologies of cognitive countermeasures employed by Western states and international institutions during the period 2022–2025.

Analysis of Recent Research and Publications. The issue of Russian information and cognitive operations targeting the West and Ukraine since 2014 has become the subject of extensive research in the fields of security studies, strategic communications, and international relations. Early scholarship focused primarily on Russian disinformation campaigns, the use of cyberattacks, and interference in electoral processes. In particular, O. Backes and A. Swab conceptualized cognitive warfare through the prism of threats to the electoral infrastructure of the Baltic states, emphasizing the systematic nature of Russian influence operations and the vulnerability of democratic institutions to the manipulation of public perception (Backes & Swab, 2019). At the institutional level, the analytical studies conducted by the RAND Corporation constitute an important source, systematizing the mechanisms of Russian information operations against Ukraine and examining the responses of Ukrainian society and civil society initiatives to these influence activities. The study Russian Social Media Influence: Understanding Russian Propaganda in Ukraine demonstrates that Ukrainian fact-checking initiatives, particularly StopFake, have played a pivotal role in exposing disinformation, countering Russian narratives, and strengthening the country's information resilience since 2014 (Helmus et al., 2018). At the same time, Eliot Higgins, drawing on the experience of Bellingcat, demonstrated how OSINT communities have reshaped the balance of trust within the information environment by creating a non-governmental yet highly evidence-based counter-narrative to Russian disinformation (Higgins, 2019).

The subsequent evolution of the discourse is associated with a shift from describing disinformation to the broader framework of cognitive operations and cognitive security. Ukrainian researcher Yu. Danyk, together with C. Briggs, considers contemporary cognitive operations an integral component of hybrid warfare, emphasizing the combination of psychological influence, information technologies, and military force (Danyk & Briggs, 2023). C. Deppe and G. Schaal conduct a conceptual analysis of NATO ACT's Cognitive Warfare Exploratory Concept initiative, demonstrating how the notion of «cognitive warfare» is gradually becoming institutionalized in Alliance documents and acquiring clearer contours within the doctrinal domain (Deppe & Schaal, 2024). B. Catena, O. Ditrych, and N. Kovalčíková, in turn, propose the concept of EU «cognitive security» as a framework for building pan-European resilience to manipulation by combining the analysis of human vulnerabilities with the assessment of technological risks (Catena, Ditrych, & Kovalčíková, 2025). These studies establish the theoretical background within which cognitive operations are regarded as a distinct domain of strategic confrontation.

Considerable attention has also been devoted to the practical effectiveness of Western cognitive countermeasures against Russian influence in the context of the war against Ukraine. T. Helmus and K. Holynska, drawing on RAND research, demonstrate that after 2022 Russian information operations experienced a substantial decline in effectiveness, while Ukrainian society displayed a high level of resilience to disinformation due to its prior wartime experience and its developed strategic communications ecosystem (Helmus & Holynska, 2024). D. Kutidze provides a detailed analysis of the transformation of Ukrainian communication practices, emphasizing the role of state institutions and civil society in shaping the narrative of resistance and developing media literacy even before the full-scale invasion (Kutidze, 2023). Hybrid CoE analysts–A. Aho and others–describe a «resilience ecosystem» against hybrid threats, in which the cognitive dimension and countering information influence are considered key elements alongside cybersecurity, energy, and critical infrastructure (Aho et al., 2023).

A separate body of scholarship focuses on the role of state institutions and international organizations in shaping cognitive countermeasures policy. NATO policy documents–the NATO Military Policy on Strategic Communications (North Atlantic Treaty Organization, 2020) and the 2022 NATO Strategic Concept (North Atlantic Treaty Organization, 2022)–recognize information and cognitive threats as a systemic security challenge. Through its Cognitive Warfare Exploratory Concept initiative and related training programmes, NATO Allied Command Transformation (ACT) promotes the integration of the cognitive dimension into military planning (NATO Allied Command Transformation, n.d.). Within the G7, the Rapid Response Mechanism, as described in the annual report of the Government of Canada, serves as a tool for coordinating responses to foreign information manipulation, including activities involving generative artificial intelligence (Government of Canada, 2023). Catena and co-authors emphasize that these institutional developments merely outline the framework of a future system of «cognitive security» which is still in the process of being established (Catena, Ditrych, & Kovalčíková, 2025).

Much of the literature also examines the technological dimension of cognitive countermeasures, particularly the role of social media platforms and artificial intelligence. Journalistic and analytical publications by A. Hern, researchers at the Digital Forensic Research Lab, and L. Rijo

document how global technology companies (Meta, Twitter/X, and Google/YouTube) detect and dismantle networks engaged in «coordinated inauthentic behavior» linked to state-sponsored influence operations, including those conducted by Russia (Digital Forensic Research Lab, 2020; Hern, 2022; Rijo, 2025). F. Pilati and T. Venturini provide a global mapping of the use of AI tools in counter-disinformation efforts, highlighting both the potential of automated monitoring and content moderation and the risks of algorithmic bias and excessive censorship (Pilati & Venturini, 2025). At the same time, analytical reports by the European Union and the G7 identify the emergence of deepfakes and generative AI models as a new level of threat in information operations (Catena, Ditrych, & Kovalčíková, 2025; Government of Canada, 2023).

The empirical evidence on public perceptions of the war and of Russia is also of particular importance to this study. The NORC/Wall Street Journal survey demonstrates an almost complete consensus among Ukrainians in viewing Russia as the principal security threat (NORC/Wall Street Journal, 2022), while data from the Pew Research Center indicate a sharp deterioration in Russia's image across leading Western countries and a sustained increase in support for Ukraine (Pew Research Center, 2023). The works of F. Chee and the statements of the High Representative of the Union for Foreign Affairs and Security Policy examine sanctions and public diplomacy as instruments of not only economic but also cognitive influence, contributing to the construction of Russia's image as a state that violates international law (Chee, 2022; High Representative of the Union for Foreign Affairs and Security Policy, 2022).

Ukrainian scholars have also made a significant contribution to the study of the cognitive dimension of contemporary military-political confrontation. Recent Ukrainian historiography has examined the institutional mechanisms for countering Russian information influence, the development of the European Union's strategic communications, the institutionalization of cognitive operations within the U.S. military-political planning system, as well as the use of historical manipulation and revisionist narratives by the Russian Federation (Bespeka, 2026a; Bespeka, 2026b; Bespeka, 2026c; Tykhomyrova, 2023; Yelova, 2025).

Despite the breadth of the existing scholarship, several aspects remain insufficiently explored. First, most studies examine individual components of the Western response–such as the activities of NATO, the European Union, the G7, technology companies, or Ukrainian institutions–whereas comprehensive studies integrating these dimensions into a unified analysis of the West's cognitive strategy during 2022–2025 remain scarce. Second, insufficient attention has been paid to how the combination of proactive measures (prebunking, intelligence declassification, and sanctions framing) and defensive measures (content moderation, fact-checking, and the promotion of media literacy) has contributed to the resilience of Ukrainian society and the long-term cohesion of allied states. Third, in the context of the rapid development of generative artificial intelligence, a more in-depth analysis is needed of how new technological tools are transforming both cognitive threats themselves and the possibilities for their neutralization. Against this background, the present article addresses this research gap by combining an examination of the institutional and technological mechanisms of Western cognitive countermeasures with an analysis of their impact on Ukraine's resilience during the full-scale Russian–Ukrainian war.

The purpose of the article is to analyze the cognitive operations and strategic mechanisms employed by Western states and international organizations to counter Russian information and psychological influence, to identify their institutional, technological, and communication instruments, and to assess how these measures contributed to the development and strengthening of Ukraine's information and psychological resilience during the period 2022–2025.

Main Body. The foundations of the Western system of cognitive countermeasures, which demonstrated its greatest effectiveness during 2022–2025, were established following the onset of Russia's aggression against Ukraine in 2014. One of the first steps was the establishment, at the initiative of NATO's Eastern European member states, of the Strategic Communications Centre of Excellence (StratCom COE) in Riga, which became a leading analytical and training hub for the study of information operations and the development of recommendations for countering disinformation. The further development of these approaches was reflected in the NATO Military Policy on Strategic Communications (2020), which defined StratCom as an integrated system for employing information and communication instruments to achieve strategic objectives (North Atlantic Treaty Organization, 2020). In the 2022 NATO Strategic Concept, Russia was officially identified as the most direct threat to Allied security, employing disinformation and other hybrid methods alongside military and cyber means (North Atlantic Treaty Organization, 2022).

Meanwhile, the European Union developed its own system for countering information influence by establishing the East StratCom Task Force and launching the EUvsDisinfo project in 2015. An important component of this system was the European Digital Media Observatory (EDMO), which, following the outbreak of the full-scale war, established a dedicated task force to analyse disinformation related to the war in Ukraine. This task force brought together researchers, fact-

checkers, and media experts from EU member states to monitor disinformation campaigns, identify their major trends, and develop recommendations for strengthening the information resilience of European societies (Tykhomyrova, 2023, pp. 95–96).

In parallel, the United States, the United Kingdom, Canada, the Baltic states, and the Nordic countries updated their information security strategies, established specialized interagency structures, and strengthened coordination in the field of countering disinformation. As a result, by the onset of the full-scale invasion, the institutional foundation of Western cognitive countermeasures had been established, integrating strategic communications, information operations, and interagency coordination into a unified system for responding to information threats (Bespeka, 2026b, pp. 90–91).

Digital platforms and independent civil society initiatives became another important component of this system. Beginning in 2016–2018, Meta, Google, and Twitter (now X) introduced mechanisms for detecting and disrupting coordinated information operations, labeling state-controlled media, algorithmically limiting the dissemination of propaganda content, and implementing other measures to counter disinformation. At the same time, a transnational network of independent OSINT researchers and fact-checkers emerged. The Bellingcat community demonstrated the effectiveness of open-source intelligence in investigating the downing of Flight MH17, the poisoning of Sergei and Yulia Skripal, and other Russian operations (Higgins, 2019). In Ukraine, with the support of Western partners, StopFake, InformNapalm, and other civil society initiatives played a significant role in documenting Russian disinformation and strengthening the country's information resilience (Helmus & Bodine-Baron, 2018). Collectively, these governmental, private-sector, and civil society initiatives formed a multi-layered system for detecting and containing information operations. Its practical implementation, particularly after the outbreak of the full-scale war, substantially reduced the ability of Russian information networks to exploit global digital platforms for conducting influence operations (Digital Forensic Research Lab, 2020; Hern, 2022; Rijo, 2025; Backes & Swab, 2019; Danyk & Briggs, 2023).

Russia’s full-scale invasion in 2022 constituted the first major test of the system of cognitive countermeasures that had been developed after 2014. From the very first days of the war, Western allies acted in a coordinated manner, seeking to shape an information agenda favourable to Ukraine and to deprive Russia of the opportunity to impose its own interpretation of events. As early as January 2022, the United States and the United Kingdom took the unprecedented step of declassifying and publicly releasing intelligence indicating that the Kremlin was preparing fabricated pretexts for the invasion (so-called false flag operations). This proactive information operation pursued two interrelated objectives: to warn the international community about the reality of the impending threat and to disrupt Moscow’s information strategy by denying it the opportunity to be the first to impose its own version of events (Helmus & Holynska, 2024).

In effect, the West conducted prebunking by exposing potential Russian provocations before they could be carried out. This disrupted the Russian Federation’s typical pattern of being the first to dominate the information space with its preferred narrative. As a result, at the outset of the invasion, Russian propaganda proved unable to provide a convincing justification for its aggression before the international community (Borger & Harding, 2022).

The success of this preventive information operation can largely be attributed to the fact that Russian cognitive influence had long been based on the systematic use of historical narratives, revisionism, and the manipulation of memory politics. Russian propaganda consistently combined modern digital technologies with historical myths about Ukraine in an effort to legitimize its aggression, cast doubt on Ukrainian statehood, and shape public perceptions of the war both within Ukraine and abroad. This required Western states not only to debunk falsehoods promptly but also to undertake the systematic historical verification of Russian manipulative narratives, which had become a significant component of contemporary cognitive confrontation (Yelova, 2025, pp. 195–197, 203–205).

Subsequently, in February–March 2022, Ukraine and its Western partners simultaneously launched large-scale communication campaigns targeting a global audience. Within a matter of weeks, a strong coalition of support had been formed: at emergency sessions of the United Nations and in statements issued by the leaders of the G7, NATO, and the European Union, Russia's aggression was unanimously condemned as unprovoked and brutal. The United Nations General Assembly Resolution of 2 March 2022, supported by 141 states (with only five voting against), clearly demonstrated the Russian Federation’s international isolation (Chee, 2022).

All these diplomatic initiatives were accompanied by consistent terminology: the aggressor was referred to as an aggressor, and the war as a war, thereby setting the tone for international information coverage. In the sphere of public consciousness, these actions can be regarded as a cognitive deterrence operation: the Kremlin failed to impose its own explanations on the international community (such as the narratives of «defence against NATO» or «denazification»); instead, the Western narrative portraying the conflict as a struggle between democracy and tyranny became dominant. Every egregious crime committed by the Russian Federation–including the shelling of cities, the killings in Bucha, and the abuse of prisoners of war–was immediately substantiated by evidence

and disseminated through global media, reinforced by statements from Western leaders. In response, Russian propagandists unsuccessfully attempted to portray the Bucha massacre as a «staged event» but credible evidence swiftly refuted these claims, thereby minimizing their impact (Aho et al., 2023).

Concurrently with the development of defensive narratives, the West intensified the use of sanctions and public diplomacy as instruments of cognitive influence. Beyond their economic impact, the imposition of stringent sanctions against the Russian Federation conveyed a clear psychological message: the international community was punishing Russia for its aggression, thereby underscoring the illegitimacy and immorality of its actions. Each new package of sanctions was accompanied by official statements emphasizing that these measures constituted a response to the bombing of cities, the atrocities committed in Bucha, and Russia's violations of international law (High Representative of the Union for Foreign Affairs and Security Policy, 2022). In this way, sanctions functioned as an instrument of war framing, reinforcing in the global consciousness the image of the Russian Federation as a state that had violated international law and was therefore being isolated and deprived of critical resources. For Ukrainian society and the Armed Forces, this served as an important signal of international support, strengthening morale by reinforcing the conviction that justice was on their side and that the international community recognized this.

Public diplomacy proved to be an equally powerful instrument. Since 2022, the leaders of the United States, the United Kingdom, the European Union, and other states have consistently articulated a message of unwavering solidarity with Ukraine. Frequent addresses to their national publics and parliaments emphasized that Ukraine's struggle was the struggle of the entire free world. The culmination of this support came in the form of President Volodymyr Zelenskyy's numerous historic speeches before the parliaments of leading countries, delivered with the support of their governments in the spring of 2022. This unprecedented direct communication of the Ukrainian narrative to Western societies strengthened the emotional connection with Ukraine and fostered a shared understanding of the objectives of the war. Visits by senior Western officials to Kyiv during periods of intense Russian shelling–including those of the President of the United States, the heads of European governments, and other high-ranking officials–produced a significant cognitive effect by clearly demonstrating the failure of the Kremlin's attempts to isolate Ukraine. These actions boosted the morale of Ukrainian society while simultaneously providing visible evidence of sustained international support for Ukraine.

As a result of these measures, Ukrainian society entered the phase of full-scale war already hardened on the information front. Regular public opinion surveys indicated a high level of awareness of the threats posed by Russia and a strong readiness to resist disinformation. According to a survey conducted by NORC at the University of Chicago in June 2022, 97% of Ukrainians identified Russia as the principal threat to their security, demonstrating an almost complete societal consensus regarding the nature of the war and a profound distrust of Russian narratives (NORC/WSJ, 2022). An analytical report by the Gnomon Wise Research Institute likewise emphasizes that, even before the full-scale invasion, Ukrainian state institutions and civil society had actively developed strategic communications aimed at enhancing media literacy and strengthening public resilience to external manipulation (Kutidze, 2023). Collectively, these factors contributed to the failure of Russian information operations to generate panic or disorient Ukrainian society; instead, Ukrainians maintained a high level of morale and national unity even during the most difficult stages of the war. At the same time, the literature notes that, despite the resilience achieved, Western approaches to cognitive countermeasures remain incomplete and require further conceptual and institutional development (Deppe & Schaal, 2024).

NATO has also gradually incorporated cognitive challenges into its military concepts. In particular, the 2021 Warfighting Capstone Concept (NWCC) identifies cognitive superiority as one of the five key imperatives of future warfare. This concept refers to the Alliance's ability to achieve a deeper understanding of the operational environment and the adversary's intentions through advanced technologies and analytical capabilities. According to the NWCC, attaining cognitive superiority encompasses the functions of out-think and out-last, underscoring the central role of the information and psychological dimension in future military operations (Pilati & Venturini, 2025).

Modern technologies and analytical systems have significantly expanded the toolkit for countering disinformation. In particular, the European Union and the United Nations have launched initiatives supporting the use of AI-based tools for monitoring and fact-checking, while private technology companies (Meta and Google) are investing in algorithms capable of automatically detecting and blocking false content. At the same time, researchers emphasize the need for the transparent and gradual deployment of such systems in order to avoid excessive censorship and algorithmic bias (Pilati & Venturini, 2025).

The rapid proliferation of generative artificial intelligence has also created new challenges. A recent EU study warns that synthetic media (deepfakes) substantially reduce the cost of producing manipulative content on a large scale (Catena, Ditrych, & Kovalčíková, 2025). During 2023–2024, this technology was increasingly employed in information operations, as documented in the annual report

of the G7 Rapid Response Mechanism, which highlights the growing threat posed by generative AI tools in the field of disinformation (Government of Canada, 2023).

At the institutional level, NATO has gone even further. Allied Command Transformation (ACT) is developing the Alliance's first concept of cognitive warfare, formally integrated into military doctrine (Pilati & Venturini, 2025). In parallel, the Cognitive Warfare Exploratory Concept initiative, coordinated by ACT, is being implemented to enhance the training and awareness of Allied personnel. The initiative facilitates civil-military cooperation, data sharing, and the development of measures aimed at strengthening cognitive resilience against external information manipulation (NATO Allied Command Transformation, n.d.). This approach envisages systematic training and coordinated action that take into account emerging technological threats in the cognitive domain.

At the strategic level, the institutionalization of multilateral cognitive countermeasures continues to advance. In particular, the G7 Rapid Response Mechanism (RRM) coordinates the efforts of member states in responding to Foreign Information Manipulation and Interference (FIMI). Its 2023 Annual Report emphasized that generative artificial intelligence had become one of the principal tools employed in FIMI operations, particularly during elections and periods of crisis (Government of Canada, 2023). At the same time, EU analysts advocate the development of a framework concept of cognitive security, envisaging the establishment of a pan-European system of cognitive resilience that incorporates both human and technological vulnerabilities into strategic planning (Catena, Ditrych, & Kovalčíková, 2025). Collectively, these initiatives indicate a growing awareness of the nature of cognitive threats and the gradual institutional adaptation of Western democracies to the challenges of information warfare. This adaptation involves incorporating the cognitive dimension into strategic planning, personnel training, resource allocation, and performance evaluation mechanisms, thereby making countering information influence a permanent component of security policy (Bespeka, 2026a).

Assessing the effectiveness of countering Russian influence, it must be acknowledged that, despite its considerable achievements, the Western strategy also has its limitations. During 2022–2023, Russian propaganda failed to undermine either the determination of the Ukrainian people to resist or the cohesion of the allied states. RAND research indicates a substantial decline in the effectiveness of Russian information operations and a high degree of international unity in support of Ukraine (Helmus & Holynska, 2024). Across European countries, public opinion became increasingly critical of Russian information sources, while support for Ukraine in some cases exceeded the initial expectations of national governments, as confirmed by international survey data (Pew Research Center, 2023). Ukraine came to be viewed with increasing frequency by Western states as a key element in safeguarding European security and the democratic order. At the same time, new institutional mechanisms were established, ranging from updated NATO approaches to countering disinformation to the strengthening of the G7 Rapid Response Mechanism, designed to ensure a rapid response to information manipulation (Government of Canada, 2023).

Within the information environment, the concept of deterrence in relation to disinformation has become firmly established, aiming to reduce the effectiveness of disinformation through the inevitability of its exposure and public rebuttal. Nevertheless, the problem remains unresolved. Russian influence operations continue to adapt to new conditions. Following the blocking of RT and Sputnik, they shifted to alternative digital platforms (mirror websites, VPNs, and Telegram), expanded their presence in regions where Western countermeasures are less developed (Africa and Latin America), and increasingly employed emerging technologies, including deepfakes and generative artificial intelligence. One important direction of this adaptation has been the intensified targeting of Western societies through the exploitation of historical and socio-political divisions. In Poland, for example, Russian propaganda systematically exploited issues such as the Volhynia tragedy, Ukrainian refugees, economic competition, and alleged Ukrainian territorial claims in an effort to undermine mutual trust among allies and weaken support for Ukraine (Yelova, 2025, pp. 203–205). The Hybrid CoE also notes that European societies continue to contain social groups vulnerable to external disinformation campaigns, a vulnerability exacerbated by domestic political polarization and socio-economic crises (Aho et al., 2023). This confirms that information resilience remains a dynamic process requiring continuous development and the timely elimination of identified vulnerabilities.

The proliferation of generative artificial intelligence has marked a new stage in the evolution of cognitive confrontation by substantially expanding the capabilities for conducting information operations. As the OECD notes, contemporary generative models enable the rapid production of large volumes of highly convincing textual, visual, audio, and video content, facilitate the large-scale dissemination of disinformation campaigns, allow messages to be tailored to different target audiences, and automate the activities of networks of fake accounts. In response, states and international organizations have begun implementing new countermeasures, including digital watermarking, content provenance systems, enhanced transparency requirements for generative models, AI risk assessment, and the application of artificial intelligence algorithms to detect synthetic media and coordinated information operations (OECD, 2024, pp. 59–60).

The use of generative artificial intelligence is fundamentally transforming the nature of cognitive confrontation, as the same technologies are increasingly being employed both to conduct information operations and to detect and neutralize them. While Russian actors use generative models to scale disinformation campaigns, produce deepfakes, and personalize manipulative content, Western states, international organizations, and digital platforms are integrating artificial intelligence algorithms into systems for the early detection of Foreign Information Manipulation and Interference (FIMI) operations, the automated analysis of information flows, and the coordination of fact-checking activities. Consequently, technological competition is gradually evolving into a process of mutual adaptation, in which the decisive advantage depends not so much on the use of artificial intelligence itself as on the speed of its integration into the institutional mechanisms of cognitive countermeasures (Government of Canada, 2023; OECD, 2024; Pilati & Venturini, 2025).

However, the effectiveness of artificial intelligence should not be overestimated. Researchers emphasize that AI algorithms may produce errors in identifying manipulative content, create risks of excessive content moderation and algorithmic bias, and undermine the balance between information security and freedom of expression (Pilati & Venturini, 2025; OECD, 2024). Under these circumstances, artificial intelligence should be regarded not as a self-sufficient instrument of cognitive countermeasures but as a component of a broader system that integrates strategic communications, expert analysis, the activities of state institutions, digital platforms, and civil society. It is precisely such an integrated model that is currently emerging within Western democracies in response to the evolving nature of contemporary cognitive threats.

Conclusions. The analysis conducted demonstrates that, during 2022–2025, Western states and international organizations developed an integrated system of cognitive countermeasures against Russian information influence, combining strategic communications, the preventive declassification of intelligence, the activities of digital platforms, OSINT communities, fact-checking organizations, sanctions-based public diplomacy, and mechanisms of international coordination. Despite certain political differences among Western partners, cooperation among the United States, the European Union, NATO, and the G7 countries in countering Russian cognitive operations remained well coordinated and ensured the effectiveness of their collective efforts. A significant outcome of these measures was the strengthening of Ukraine's information resilience, which, combined with the support of international partners, limited the Russian Federation's ability to impose its information narratives on both Ukrainian society and the international community. At the same time, Russian influence operations continue to adapt to evolving conditions through the active use of generative artificial intelligence, alternative digital platforms, and the exploitation of internal divisions within Western societies. This highlights the need for the further institutionalization of cognitive security, enhanced international coordination, and the continuous refinement of mechanisms for detecting and countering contemporary cognitive threats.**Funding.** The author received no financial support for the conduct of this research.

References:

Aho, A., Alonso Villota, M., Giannopoulos, G., Jungwirth, R., Lebrun, M., Savolainen, J., Smith, H., Willkomm, E. (2023). Hybrid Threats: A Comprehensive Resilience Ecosystem. *European Centre of Excellence for Countering Hybrid Threats*. URL: https://www.hybridcoe.fi/publications/hybrid-threats-a-comprehensive-resilience-ecosystem/ [in English].

Backes, O., & Swab, A. (2019). Cognitive Warfare: The Russian Threat to Election Integrity in the Baltic States. *Belfer Center for Science and International Affairs*. URL: https://www.belfercenter.org/publication/cognitive-warfare-russian-threat-election-integrity-baltic-states [in English].

Bespeka, V. (2026a). Institutionalization of Cognitive Operations in the U.S. Military-Political Planning System (2001–2025). *Visnyk humanitarnykh nauk*, 16. https://doi.org/10.5281/zenodo.18850203 [in Ukrainian].

Bespeka, V. (2026b). Retrospective Analysis of the Activities of Western States and International Organizations in Countering the Cognitive Influence of the Russian Federation (2014–2025). *Voienno-istorychnyi visnyk*, 60(2), 88–95. https://doi.org/10.33099/2707-1383-2026-60-2-88-95 [in Ukrainian].

Bespeka, V. (2026c). Russian propaganda narratives against Ukraine: cognitive structure and strategic functions (2014–2025). *Scientific Papers of the Vinnytsia Mykhailo Kotsyiubynskyi State Pedagogical University Series History*, 55, 195-205. https://doi.org/10.31652/2411-2143-2026-55-195-205 [in Ukrainian].

Borger, J., & Harding, L. (2022). US Claims Russia Planning 'False-Flag' Operation to Justify Ukraine Invasion. *The Guardian*, 14 January. URL: https://www.theguardian.com/world/2022/jan/14/us-russia-false-flag-ukraine-attack-claim [in

English].

Catena, B., Ditrych, O., & Kovalčíková, N. (2025). Smoke and Mirrors: Building EU Resilience Against Manipulation Through Cognitive Security. *EU Institute for Security Studies*, 7 October. URL: https://www.iss.europa.eu/publications/briefs/smoke-and-mirrors-building-eu-resilience-against-manipulation-through-cognitive [in English].

Chee, F. Y. (2022). EU Bans RT, Sputnik over Ukraine Disinformation. *Reuters*, 2 March. URL: https://www.reuters.com/world/europe/eu-bans-rt-sputnik-banned-over-ukraine-disinformation-2022-03-02/ [in English].

Danyk, Y., & Briggs, C. M. (2023). Modern Cognitive Operations and Hybrid Warfare. *Journal of Strategic Security*, 16(1), 35–50. https://doi.org/10.5038/1944-0472.16.1.2032 [in English].

Deppe, C., & Schaal, G. S. (2024). Cognitive Warfare: A Conceptual Analysis of the NATO ACT Cognitive Warfare Exploratory Concept. *Frontiers in Big Data*, 7, Article 1452129. https://doi.org/10.3389/fdata.2024.1452129 [in English].

Digital Forensic Research Lab. (2020). Twitter Botnet Targeted Turkey While Politicizing Coronavirus. *Atlantic Council*, 2 April. URL: https://dfrlab.org/2020/04/02/twitter-botnet-targeted-turkey-while-politicizing-coronavirus [in English].

Government of Canada. (2023). G7 Rapid Response Mechanism Annual Report 2023. *Global Affairs Canada*. URL: https://international.gc.ca/transparency-transparence/rapid-response-mechanism-mecanisme-reponse-rapide/2023-annual-report-rapport-annuel.aspx?lang=eng [in English].

Helmus, T. C., & Holynska, K. (2024). Ukrainian Resistance to Russian Disinformation: Lessons for Future Conflict. *RAND Corporation*. URL: https://www.rand.org/pubs/research_reports/RRA2771-1.html [in English].

Helmus, T. C., Bodine-Baron, E., Radin, A., Magnuson, M., Mendelsohn, J., Marcellino, W., Bega, A., & Winkelman, Z. (2018). Russian Social Media Influence: Understanding Russian Propaganda in Ukraine. RAND Corporation. URL: https://www.rand.org/pubs/research_reports/RR2237.html [in English].

Hern, A. (2022). Meta Takes Down 'Influence Operations' Run by China and Russia. *The Guardian*, 27 September. URL: https://www.theguardian.com/technology/2022/sep/27/meta-takes-down-influence-operations-run-by-china-and-russia [in English].

Higgins, E. (2019). *We Are Bellingcat: An Intelligence Agency for the People*. London: Bloomsbury. [in English].

High Representative of the Union for Foreign Affairs and Security Policy. (2022). Declaration on Russian Atrocities Committed in Bucha and Other Ukrainian Towns. *Council of the European Union*, 4 April. URL: https://www.consilium.europa.eu/en/press/press-releases/2022/04/04/ukraine-declaration-by-the-high-representative-on-behalf-of-the-eu-on-russian-atrocities-committed-in-bucha-and-other-ukrainian-towns/ [in English].

Kutidze, D. (2023). Ukraine's Strategic Communication Against Russian Disinformation. *Gnomon Wise Research Institute*. URL: https://gnomonwise.org/public/storage/publications/October2023/mOEblCoTHtfxaBp8ql6p.pdf [in English].

NATO Allied Command Transformation. (n.d.). Protecting the Alliance Against the Threat of Cognitive Warfare [Video]. *NATO ACT*. URL: https://www.act.nato.int/activities/cognitive-warfare [in English].

Norc/Wall Street Journal. (2022). Ukraine Survey. *NORC at the University of Chicago.* URL: https://s.wsj.net/public/resources/documents/WSJ_NORC_Ukraine_Poll_June_2022.pdf [in English].

North Atlantic Treaty Organization. (2020). *NATO Military Policy on Strategic Communications* (MC 0628). URL: https://www.act.nato.int/wp-content/uploads/2023/06/nato-pao-handbook-2020.pdf [in English].

North Atlantic Treaty Organization. (2022). *NATO 2022 Strategic Concept: Adopted by Heads of State and Government at the NATO Summit in Madrid*, 29 June 2022. URL: https://www.nato.int/content/dam/nato/webready/documents/publications-and-reports/strategic-concepts/2022/290622-strategic-concept.pdf [in English].

Pew Research Center. (2023). *Overall Opinion of Russia*. 10 July. URL: https://www.pewresearch.org/global/2023/07/10/overall-opinion-of-russia/ [in English].

Pilati, F., & Venturini, T. (2025). The Use of Artificial Intelligence in Counter-Disinformation: A World Wide (Web) Mapping. *Frontiers in Political Science*, 7. https://doi.org/10.3389/fpos.2025.1517726 [in English].

Rijo, L. (2025). Google Terminates Over 18,500 Channels in Q3 2025 Influence Operations. *PPC Land*, 15 November. URL: https://www.ppc.land/google-terminates-over-18-500-channels-in-q3-2025-influence-operations/ [in English].

Tykhomyrova, Ye. (2023). EU Strategic Communications on Trends in Russian Disinformation During the Full-Scale Russian-Ukrainian War. *Mizhnarodni vidnosyny, suspilni komunikatsii ta rehionalni studii,* 1(15), 91–105. https://doi.org/10.29038/2524-2679-2023-01-91-105 [in Ukrainian].

Yelova, T. (2025). Information Manipulation and Revisionist Narratives of the Russian Federation as Challenges to the Resilience of European Societies. *Mizhnarodni vidnosyny, suspilni komunikatsii ta rehionalni studii,* 4(24), 195–220. https://doi.org/10.29038/2524-2679-2025-04-195-220 [in Ukrainian].

Надійшла до редакції / Received: 25.03.2026 Схвалено до друку / Accepted: 03.06.2026