

Information as a tool of cognitive warfare in the context of hybrid warfare

TOMASZ GERGELEWICZ

Higher School of Safety and Security Services in Warsaw



<https://orcid.org/0000-0002-9145-5099>

Abstract

Information has become a powerful weapon, comparable to traditional means of warfare. The development of technology along with societies' susceptibility to harmful narratives facilitates hostile information activities, which in the cognitive domain may lead to cognitive warfare. The aim of this article is to systematise and characterise the concepts related to this warfare. The main research problem can be summarised as follows: what role does information play in hostile activities carried out in the cognitive domain? The research process is based on an analysis of Polish and English literature, professional sources, and social media.

Keywords

cognitive warfare, information warfare, hybrid warfare, dis-information, psychological warfare

Introduction

Information has become a weapon in the hands of aggressors and can be just as dangerous as traditional means of warfare. Development of modern technologies and society that accepts information uncritically mean that cognitive war¹ can be seen as an effective mechanism for hostile influence.

To understand harmful actions in a cognitive domain, it is necessary first and foremost to understand the role of information. That is why the author set out to systematise the concepts relating to cognitive warfare. He covers issues relating to, among others, hybrid threats, information environment, information operations and psychological activities as well as disinformation. He notices that concepts such as: disinformation, information operations, fake news and manipulation are used too often in a public space as synonyms. Furthermore, the term ‘hybrid war’ is overused.

The aim of the article is to answer the question: how is the information used in hostile activities within cognitive domain? The article is based on analytical method, which was used to identify specific areas of significance in the discourse on the role of information in war, and a synthetic method, applied to highlight the points of convergence between these areas and the cause-and-effect relationship between information and cognitive warfare.

The issue of the use of information for the purpose of conducting hostile activities is a recurring theme in public and academic discourse both at home and abroad. The source material therefore comprises both Polish- and English-language literature on the subject. Industry-specific websites and social media were also used as sources, as expert knowledge in this field is not always available in academic publications.

Information environment

Understanding of issues relating to information and information environment is essential for an in-depth discussion of cognitive warfare. Wiesław Flakiewicz points out that information is (...) *a factor that enhances our understanding of the world around us*². Information has also become a weapon, while the information

¹ For more information, see the subchapter: *Cognitive warfare*.

² Fraś J., *Zarządzanie informacją elementem budowy przewagi konkurencyjnej e-przedsiębiorstwa* (Eng. Information management as the key component in creating a competitive edge in e-business), “Studia i Prace Wydziału Nauk Ekonomicznych i Zarządzania” 2011, no. 21, p. 32.

environment – the space in which society operates – has become a battlefield. Thus, in the context of this discussion, information is regarded as a resource of specific data that can be used as a weapon in information environment.

The information environment consists of several components. Adam Łapszyński points out that these are: (...) *information itself, those (individuals and organizations) who receive, process and convey it as well as the space in which it occurs*³. He refers to communication in which one can identify, among other things, the sender, the recipient, the information and the space. Marc J. Romanych claims that information environment is (...) *the aggregate of individuals, organizations, or systems that collect, process, or disseminate information; also included is information itself*⁴. In this case, an analogy can be drawn with the information or intelligence cycle, in which information is obtained, gathered, processed and disseminated⁵. The National Security Bureau (BBN) emphasises the importance of the information environment as a key component in national security planning. It highlights areas of information environment such as, among others, cybersecurity, strategic communication and cognitive security⁶.

With regard to information environment, it is worth to explain what information space is. It is defined, among others, as a discontinuous and heterogeneous collection of information sources – (...) *the objects (real or virtual) to which the individual turns to acquire information*⁷. Małgorzata Kisilowska states that information space is a multidimensional, dynamic, open collection of content (data and information), its carriers and users⁸.

In the discourse on the information environment and the information space, infosphere should also be taken into account. According to Michale Vlahos, it

³ A. Łapszyński, *Monitoring the Information Environment In the Baltic Sea Region*, "The Baltic Amber. Multinational Corps Northeast Magazine" 2020.

⁴ M.J. Romanych, *Visualizing the Information Environment*, "Military Intelligence Professional Bulletin" 2003, vol. 29, no. 3, p. 5.

⁵ See in more detail: L. Dalinczuk, *Analiza wywiadowcza jako ważny element bezpieczeństwa narodowego* (Eng. Analysis as an important element of national security), in: *Współczesne zagrożenia bezpieczeństwa państwa cz. II*, Z. Ciekanowski (sci. ed.), Biała Podlaska 2021, pp. 176–183.

⁶ *Biuro Bezpieczeństwa Narodowego 2015–2025* (Eng. National Security Bureau 2015–2025), <https://www.bbn.gov.pl/pl/informacje-o-bbn/publikacje/10209,Biuro-Bezpieczenstwa-Narodowe-2015-2025.html>, p. 52 [accessed: 28 IX 2026].

⁷ C. McKnight, *The Personal Construction of Information Space*, "Journal of the American Society for Information Science" 2000, vol. 51, no. 8, p. 730. [https://doi.org/10.1002/\(SICI\)1097-4571\(2000\)51:8<730::AID-ASI50>3.0.CO;2-8](https://doi.org/10.1002/(SICI)1097-4571(2000)51:8<730::AID-ASI50>3.0.CO;2-8).

⁸ M. Kisilowska, *Przestrzeń informacyjna jako termin informatologiczny* (Eng. Information space as an information science term), "Zagadnienia Informatyki Naukowej – Studia Informacyjne" 2011, no. 2, pp. 35–52. <https://doi.org/10.36702/zin.666>.

is (...) *the fusion of all the world's communications networks, databases and sources of information into a vast, intertwined and heterogeneous tapestry of electronic interchange*⁹. Luciano Floridi also raised this issue. According to him, infosphere (...) *is the whole informational environment constituted by all informational entities (thus including informational agents as well), their properties, interactions, processes and mutual relations. It is an environment comparable to, but different from cyberspace (which is only one of its sub-regions, as it were)*¹⁰. Referring to a cyberspace, Mirosław Karpiuk points out that (...) *the speed, accessibility and limited accountability associated with the circulation of information in cyberspace make it the area of the infosphere that is ideally suited for the transmission of false content*¹¹.

The aim of defining these concepts is to facilitate an understanding of the information battlefield. The author points out that, for the purposes of addressing the research problem, the information space and the infosphere must be reduced to a common semantic denominator and identified as the elements of information environment.

Information environment in which information intertwines carries with it a variety of risks. The malicious use of information in the course of carrying out information operations (infoops) may lead to information warfare. It (...) *aims to disrupt leadership, mislead enemies, form desirable public opinions/perceptions, organize anti-government activities, and decrease the enemy's will, often considering influence and technical aspects as a unified whole*¹². Andrew Borden points out that it (...) *is any action to Deny, Exploit, Corrupt or Destroy the enemy's information and its functions; protecting ourselves against those actions and exploiting our own military information function*¹³. As set out in the Defence Concept of the Republic of Poland (...) *although wars will continue to be waged primarily by kinetic means in the future, other methods of warfare will also gain in importance. Cyberspace and the information battlefield are already becoming a new kind of front line*¹⁴.

⁹ M. Vlahos, *Entering the Infosphere*, "Journal of International Affairs" 1998, vol. 51, no. 2, p. 498.

¹⁰ L. Floridi, *A Look into the Future Impact of ICT on our Lives*, "The Information Society" 2007, vol. 23, no. 1, p. 59. <https://doi.org/10.1080/01972240601059094>.

¹¹ W.M. Karpiuk, *The Cybersecurity Strategy of the Republic of Poland as a Source of Internal Law*, "Cybersecurity and Law" 2024, no. 2, p. 235.

¹² M. Calkayis, *Contemporary Information Warfare, Artificial Intelligence, and Challenges for Democracies*, NAVI, 26 X 2025, <https://nato-veterans.org/contemporary-information-warfare-artificial-intelligence-and-challenges-for-democracies/> [accessed: 6 XI 2025].

¹³ A. Borden, *What Is Information Warfare?*, <https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Chronicles/borden.pdf>, p. 1 [accessed: 20 V 2024].

¹⁴ *Koncepcja Obronna Rzeczypospolitej Polskiej* (Eng. The Defence Concept of the Republic of Poland), Ministerstwo Obrony Narodowej, Warszawa 2017, pp. 36–37.

In summary, information environment – in the context of the present discussion – should be regarded as a space shared by information that may be used for hostile information operations.

Disinformation

As part of hybrid activities, information operations and psychological influence are used to employ tools designed to exert a negative influence on the target group. Some of the most effective measures in this regard are: the use of false information, so-called ‘fake news’, the manipulation of facts and the creation of information noise, all of which constitute the process of disinformation¹⁵. The author deliberately defines disinformation as a process, as it involves elements of informational and psychological influence that the aggressor uses in a manner planned across time and space in order to achieve specific objectives.

Instructions of the second Department of the General Staff of the Polish Army of May 1926 explains that disinformation is (...) *providing the enemy's intelligence service with information designed to conceal one's own intentions (...) and forcing it to treat information provided by one's own intelligence service as true, or forcing the enemy's intelligence service to analyse fabricated reports*¹⁶. Experts from the Kościuszko Institute state that (...) *disinformation is the deliberate creation and dissemination of false information with the aim of manipulation. The key element of disinformation is deliberateness and awareness*¹⁷. According to Richard Deacon, disinformation consists of fabricated testimonies, slander tactics and forged documents used to discredit an opponent¹⁸. Disinformation was also described as a form of deception carried out to gain tactical and strategic advantages: in terms of image, politics, finance and military matters¹⁹. According to Robert Nogacki and Krzysztof Surdyk, the term ‘disinformation’ should also be understood to include a method of concealment involving the deliberate dissemination of false

¹⁵ The term appeared in spring of 1926 in the London monthly magazine *The Whitehall Gazette & St. James's Review*.

¹⁶ A. Peplowski, *Wojna o tajemnice. W tajnej służbie Drugiej Rzeczypospolitej 1918–1944* (Eng. *The War for Secrets. The Secret Service of the Second Polish Republic 1918–1944*), Kraków 2011, p. 335.

¹⁷ *Z tarczą! Jak chronić się przed dezinformacją?* (Eng. *With a shield! How can you protect yourself from disinformation?*), K. Mikulski, M. Krawczyk (eds.), Kraków 2021.

¹⁸ *Disinformation*, in: R. Deacon, *Spyclopedia*, London 1989, p. 400.

¹⁹ I.M. Pacepa, R.J. Rychlak, *Dezinformacja. Były szef wywiadu ujawnia metody dławienia wolności, zwalczania religii i wspierania terroryzmu* (Eng. *Disinformation. Former intelligence chief reveals methods used to stifle freedom, suppress religion and support terrorism*), Gliwice 2015.

information about the object being concealed, its structure and its activities. They point out that disinformation encompasses conducting special operations and activities aimed at concealing secrets, misleading the enemy on matters relating to political, economic, scientific, technical and military issues, as well as inducing the enemy to take decisions and actions that would be advantageous to the party engaging in the deception²⁰.

The Great Soviet Encyclopaedia defines disinformation as (...) *the dissemination through press and radio of false data with the purpose of misleading public opinion*²¹. According to *Espionage: An Encyclopedia of Spies and Secrets*, disinformation is (...) *the creation and dissemination of misleading or false information with the aim of damaging the country's reputation*²². The European Parliament states that disinformation is:

(...) deliberately manipulated content, spread to deceive or fool an audience and achieve strategic, political, or economic goals. It is often spread by malign actors who aim to undermine trust in democratic institutions or influence elections. Disinformation is dangerous for democracy because it distorts public debate, polarises society and hinders people's ability to make informed choice free from interference and manipulation²³.

Another definition points out that disinformation is (...) *the deliberate dissemination of false or misleading information with a view to achieving specific objectives, such as manipulating public opinion, undermining confidence in institutions or causing confusion. Disinformation can take various forms, such as fake news, conspiracy theories, misrepresentations or exaggerations of the facts*²⁴. Katarzyna Bąkowicz states that (...) *disinformation is sometimes deliberately disseminated to achieve objectives set by the sender, often using channels that accelerate its dissemination*

²⁰ R. Nogacki, K. Surdyk, *Teoria i praktyka działań dezinformacyjnych* (Eng. The theory and practice of disinformation campaigns), Profesjonalny Wywiad Gospodarczy Skarbiec, 19 II 2020, <https://www.wywiad-gospodarczy.pl/teoria-i-praktyka-dzialan-dezinformacyjnych.html> [accessed: 19 VIII 2025].

²¹ A. Golitsyn, *New Lies For Old. The Communist Strategy of Deception And Disinformation*, New York 1984.

²² *Disinformation*, in: R.M. Bennett, *Espionage: An Encyclopedia of Spies and Secrets*, London 2002, p. 69.

²³ *Disinformation: 10 steps to protect yourself and others*, European Parliament, 11 VI 2025, <https://www.europarl.europa.eu/topics/en/article/20250603STO28720/disinformation-10-steps-to-protect-yourself-and-others> [accessed: 21 X 2025].

²⁴ *Wykorzystanie sztucznej inteligencji w wykrywaniu dezinformacji w Internecie* (Eng. The use of artificial intelligence in detecting disinformation on the internet), Serwis Rzeczypospolitej Polskiej, 10 VIII 2023, <https://www.gov.pl/web/5g/wykorzystanie-sztucznej-inteligencji-w-wykrywaniu-dezinformacji-w-internecie> [accessed: 27 X 2025].

and extend its reach to a wide audience. This is a strategic and carefully planned initiative aimed at achieving results, involving all elements of information process²⁵. As stated in 'Przegląd Nauk o Obronności' (Defence Science Review), disinformation poses a direct threat to national security and may influence defence policy, including its strategic objectives relating to ensuring independence. Furthermore, it may interfere with democratic processes, leading to the undermining of the state's stability and to malfunctions in the operation of public authorities²⁶.

Sun Tzu, a theorist of the art of war, wrote in his treatise 'The Art of War' that, in wartime, victory without a fight is the most important skill: (...) *all warfare is based on deception. Hence, when able to attack, we must seem unable; when using our forces, we must seem inactive; when we are near, we must make the enemy believe we are far away* (...) ²⁷. Vladimir Volkoff, a former French Intelligence officer, described disinformation as an action aimed at legitimising hostile ideas among members of the targeted societies. In such cases, it is carried out systematically, using the mass media, and is directed at public opinion. Furthermore, he pointed out that disinformation is aimed at altering the course of events and is linked to the destabilisation of the enemy's society²⁸. According to NASK: (...) *the ultimate aims of disinformation are to instil fear, erode trust in institutions and cause social polarisation* (...). *Disinformation undermines trust in public institutions, science and the media. It contributes to the destabilisation of the state and fuels social divisions*²⁹. The Police also report that disinformation (...) *refers to false or misleading content, which may take the form of posts, articles, videos or audio recordings. Its aim is to deliberately cause harm to the public or to make a profit*³⁰.

The North Atlantic Alliance devotes a great deal of attention to disinformation and strategies for combating it. The NATO 2022 Strategic Concept

²⁵ Bąkowicz K., *Praktyczne rozumienie dezinformacji wśród polskich przedsiębiorstw: obszary i tendencje* (Eng. Practical understanding of disinformation among Polish enterprises: areas and trends), "Zeszyty Naukowe Akademii Górnośląskiej" 2023, no. 10, pp. 127–137. <https://doi.org/10.53259/2023.10.13>.

²⁶ K. Kaczmarek, M. Karpiuk, C. Melchior, *Disinformation as a Threat to State Security*, "Przegląd Nauk o Obronności" 2024, no. 20, p. 47. <https://doi.org/10.37055/pno/205780>.

²⁷ S. Tzu, *The Art of War*, https://ebook-mecca.com/online/The_Art_of_War.pdf, p. 8 [accessed: 27 IX 2025].

²⁸ Volkoff V., *Psychosocjotechnika. Dezinformacja. Oręż wojny* (Eng. psychosocial engineering. Disinformation. Weapon of war), Warszawa 1991.

²⁹ *Chroń się przed dezinformacją* (Eng. Defend yourself against disinformation), NASK, <https://www.nask.pl/instytut/dla-ciebie/dezinfo> [accessed: 19 IX 2025].

³⁰ *Czy wiesz jak chronić się przed dezinformacją?* (Eng. Do you know how to defend yourself against disinformation?), Komenda Powiatowa Policji w Oławie, 24 XI 2024, <https://olawa.policja.gov.pl/doa/aktualnosci/bieza/132251,Czy-wiesz-jak-chronic-sie-przed-dezinformacja.html> [accessed: 15 IX 2025].

lists the most significant threats, particularly from Russia, which NATO must address. The document emphasised the need to invest in deterrence and defence capabilities against political, economic, energy and information coercion, as well as other hybrid tactics³¹. The Allied Command Transformation (ACT) states that (...) *various external actors are trying to undermine the unity of the alliance and affect our populations (...). Disinformation campaigns, fake news or conspiracy theories are used to fragment states and polarise their public opinion*³². The Special Report of the European Court of Auditors points out that (...) *disinformation is a serious concern in organised societies. Social media and new technologies have increased the scale and speed with which false or misleading information can reach its audiences, whether intended and unintended*³³. The European Commission communication on the scale and scope of disinformation identified several reasons for its spread, such as: rapid cultural, social and economic shifts, which generate, among other things, rise in social tensions, media transformation and the popularity of online platforms³⁴. As Bąkiewicz claims, the ease with which disinformation spreads is also influenced by factors that contribute to the public's irresponsible attitude towards information, such as: the selectivity of human perception, a lack of interest in reliable information, and people's unquestioning trust in the authority of others that reduces critical thinking³⁵.

It is worth noting the difference between disinformation and misinformation. The latter is defined as false content, created without malicious intent, which is misleading as a result of, for example, a lack of knowledge or a confusion of facts. The party providing the misinformation usually believes that they are conveying accurate information³⁶.

An example of a state that spreads disinformation on a large scale is the Russian Federation. The Defence Concept of the Republic of Poland states that (...) *Russian*

³¹ NATO 2022 Strategic Concept, NATO, 29 VII 2022, <https://www.nato.int/en/about-us/official-texts-and-resources/strategic-concepts/nato-2022-strategic-concept> [accessed: 9 XII 2024].

³² *Protecting the Alliance Against the Threat of Cognitive Warfare*, YouTube, 9 V 2023, <https://www.youtube.com/watch?v=4Pn57uoyYEA> [accessed: 5 XI 2025].

³³ *Disinformation affecting the EU: tackled but not tamed. Special report*, https://www.eca.europa.eu/Lists/ECADocuments/SR21_09/SR_Disinformation_EN.pdf [accessed: 15 X 2025].

³⁴ J. Balcewicz, *Zwalczanie dezinformacji w internecie: podejście europejskie* (Eng. Combating disinformation online: European approach), Cyberpolicy NASK, 26 IV 2018, <https://cyberpolicy.nask.pl/zwalczanie-dezinformacji-w-internecie-podejscie-europejskie> [accessed: 17 X 2025].

³⁵ K. Bąkiewicz, *Praktyczne rozumienie dezinformacji...*

³⁶ Tomala L., *Kto wierzy w fake newsy? Badacze chcą zwalczać szkodliwe informacje jak epidemie* (Eng. Who believes in fake news? Researchers want to combat harmful information as if it were an epidemic), *Nauka w Polsce*, 7 II 2021, <https://naukawpolsce.pl/aktualnosci/news%2C86178%2Ckto-wierzy-w-fake-newsy-badacze-chca-zwalczac-szkodliwe-informacje-jak> [accessed: 15 X 2025].

*policy is closely coordinated with operations of the special services, including active measures taken against others states*³⁷. The Kremlin runs disinformation campaigns, which are intended not only to conceal Russia's current activities from its own citizens, but above all to establish a manipulated permanent image of NATO as an offensive alliance³⁸. In the Russian concept of next-generation warfare, a typical armed conflict must always be preceded by political, informational and psychological rivalry, during which there is ample scope to influence the opponent, undermine their morale and thereby reduce their will to fight, as well as to portray them as responsible for the escalation³⁹. Valery Gerasimov stated that (...) *the role of nonmilitary means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness*⁴⁰. Hostile activities within the Russian information space include, among other things: undermining the credibility of states on the international stage and portraying them as Russophobic, as well as weakening their position within the EU and NATO on the issue of policy towards the Kremlin⁴¹.

According to Michał Oleksiejuk, Russia is projecting an image of itself as a state under threat and destabilised by external forces. As a result, the Russian public is to be convinced that Russia is a besieged fortress⁴². Olga Wasiuta and Sergiusz Wasiuta note that Russia does not respect the independence of its neighbours, and employs tactics such as disinformation campaigns, economic intimidation and religious tensions⁴³. The authors write that (...) *in recent years, Russia has increased the capabilities of all branches of its armed forces, is expanding its electronic warfare systems, intelligence and cyber capabilities, as well as its space programmes; it*

³⁷ *Koncepcja Obronna Rzeczypospolitej Polskiej...*, p. 23.

³⁸ *Dlaczego obca propaganda jest skuteczna w obszarze obronności?* (Eng. Why is foreign propaganda effective in the field of defence?), Stop Fake Org, 5 VIII 2019, <https://www.stopfake.org/pl/dlaczego-obca-propaganda-jest-skuteczna-w-obszarze-obronnosci/> [accessed: 29 X 2025].

³⁹ M. Wojnowski, *Koncepcja „wojny nowej generacji” w ujęciu strategów Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej* (Eng. The concept of 'modern warfare' formulated by strategists of the Russian Federation Armed Forces Headquarters), "Przegląd Bezpieczeństwa Wewnętrznego" 2015, no. 13, pp. 13–39.

⁴⁰ T. Ołowski, *Rosyjskie myślenie o wojnie* (Eng. The Russian perspective on war), "Polska Zbrojna" 2021, no. 5, p. 82.

⁴¹ Z. Zielonka, K. Rumiński, *Poland Place of Freedom*, Ministerstwo Obrony Narodowej, Warszawa 2017, p. 47.

⁴² M. Oleksiejuk, *Dangerous Russian Siege Mentality*, Warsaw Institute, 31 VIII 2020, <https://warsawinstitute.org/dangerous-russian-siege-mentality/> [accessed: 29 VIII 2025].

⁴³ *Encyklopedia Bezpieczeństwa* (Eng. Encyclopaedia of security), vol. 5, O. Wasiuta, S. Wasiuta (eds.), <https://inob.uken.krakow.pl/wp-content/uploads/sites/37/2023/10/Encyklopedia-tom-5.pdf> [accessed: 2 XII 2025].

is militarising the Kaliningrad region, influencing the political debate in the NATO and EU states, and fuelling polarisation of the societies (...) ⁴⁴. In their research into Russian activities on the Telegram and X social media platforms, Jean-Christophe Boucher and Ofer Fridman point to large-scale foreign information manipulation and interference (FIMI) ⁴⁵ carried out by the Kremlin, which were tailored to specific target groups in selected countries ⁴⁶. In her conclusions from the content analysis on the Sputnik platform, Katarzyna Kwiatkowska-Moskalewicz states that (...) *'the parasite strategy' adopted by Russia involves copying and adopting Western models whilst giving them a contrasting set of meanings* ⁴⁷. In view of the above, it should be emphasised that, in the 21st century, the RF became a case study of a state pursuing a hostile imperialist policy based largely on hybrid operations on an unprecedented scale.

The author notes that disinformation comprises three tools of information influence: false information, so-called fake news, manipulation of facts and information noise. The first tool encompasses information that has been created with the intention of misleading and is disseminated, either deliberately or accidentally ⁴⁸. Fake news, when taken in the right context, may appear to have the characteristics of genuine information. The second tool is the manipulation of facts, namely (...) *taking advantage of certain circumstances, bending or distorting the facts in order to prove one's point or to influence other people's views and behaviours* ⁴⁹. Manipulation used for the purpose of disinformation is particularly dangerous because it is difficult to verify. In turn, information noise, involves generating a large amount of contradictory or similar information. This makes it easier to lend credibility to fake news, encourages the manipulation of facts and distracts the user of infosphere. The recipient loses the ability to determine what they should focus on and how to assess the value of individual pieces of information. Paulina Piasecka points out

⁴⁴ Ibid.

⁴⁵ This is a concept proposed by the European External Action Service with a view to fostering a discourse on external hostile information influence. See in more detail: *Creation of the European External Action Service*, European Union External Action, 19 VIII 2021, https://www.eeas.europa.eu/eeas/creation-european-external-action-service_en [accessed: 20 XII 2025].

⁴⁶ *Counter-FIMI Toolbox for Diplomats. A Conceptual Framework*, <https://community-democracies.org/app/uploads/2025/01/Counter-FIMI-Toolbox.pdf>, p. 6 [accessed: 2 IX 2026].

⁴⁷ K. Moskalewicz-Kwiatkowska, *Pasożytnicza strategia rosyjskiej propagandy* (Eng. Parasite strategy of Russian propaganda), Warszawa 2024.

⁴⁸ *Rozpoznawanie nieprawdziwych informacji* (Eng. Identifying false information), Serwis Rzeczypospolitej Polskiej, <https://www.gov.pl/web/baza-wiedzy/roznpoznanawanie-nieprawdziwych-informacji> [accessed: 20 III 2023].

⁴⁹ Search term: manipulation, *Słownik języka polskiego* (Eng. Dictionary of the Polish Language), <https://sjp.pwn.pl/sjp/manipulacja;2481186> [accessed: 10 IX 2025].

that information noise involves flooding the information space with ubiquitous and unauthorised information. During offensive activities, that sort of noise can effectively conceal the aggressor's targets and actions⁵⁰.

The media play an important role in shaping the narrative and generating information noise. As Chiara de Franco states: (...) *the narratives produced by the media, especially by those constructed around one or more images, do create a reality effect which impacts not only the public at large, but also on policymakers. Those narratives constitute a mediated reality which interferes with the policymaking process because they affect the mental image of a given issue through which policymakers interact and on the basis of which they take decisions*⁵¹. That is why the media should provide a forum for credible and reliable information, and act as an impartial and independent source that meets high ethical standards⁵².

In summary, disinformation should be regarded as a hostile and deliberate process of using fake news, manipulated facts and information noise to force a misjudgement of reality and lead to decisions being taken in line with the aggressor's will.

Psychological warfare

When describing hybrid warfare, the concept of psychological operations (psyops) should be discussed, as they constitute the essence of tools of influence in the cognitive domain. NATO defines psychological operations as: (...) *planned psychological activities using methods of communications and other means directed to approved audiences in order to influence perceptions, attitudes and behaviour, affecting the achievement of political and military objectives*⁵³. Psychological operations can be viewed within the framework of psychological warfare, which points, among other things, to more diverse objectives – including political and strategic ones – a deeper scope of action, a longer duration and a wider range of measures employed to carry it out.

⁵⁰ N. Gorzelnik, *Twój post na fejsie może kosztować życie. Oto jak wrogie wywiady wykorzystują social media* (Eng. Your Facebook post could cost someone their life. Here's how hostile intelligence services exploit social media), INN Poland, 28 III 2022, <https://innpoland.pl/177769,jak-twoje-dzialania-w-sieci-wspieraja-rosyjski-wywiad> [accessed: 28 VIII 2024].

⁵¹ C. de Franco, *Media Power and the Transformation of War*, New York 2012, p. 47.

⁵² *Recommendations of the Committee of Ministers to member states on the remit of public service media in the information society* (Adopted by the Committee of Ministers on 31 January 2007 at the 985th meeting of the Ministers' Deputies), CM/Rec (2007)3, <https://search.coe.int/cm/?i=09000016805d-6bc5> [accessed: 14 IX 2025].

⁵³ NATO, *Allied Joint Doctrine for Psychological Operations*, AJP-3.10.1(A), 2007, 1-1.

According to the definition in *the Dictionary of the Polish Language*, psychological warfare is (...) *the deliberate exertion of pressure on a particular state by means of ideological propaganda, threats and intimidation*⁵⁴. *The Great Dictionary of the Polish Language* defines psychological warfare as (...) *exerting pressure on a country, organisation or a group through threats, intimidation or hostile propaganda*⁵⁵. Another definition refers to a set of activities (...) *based on comprehensive knowledge of the spectrum of human behaviour and characterised by the use of tools and measures that influence social behaviour, with a view to creating opportunities for social control – understood as the ability to persuade a given population to achieve specific objectives*⁵⁶. In the *Information Security Handbook*, a service is defined as (...) *the systematic use of propaganda and related public information measures to influence public opinion, the feelings, attitudes and behaviour of the enemy and foreign groups, so as to assist in the implementation of the state's policies, objectives and military tasks*⁵⁷. As Marcin Olechowski writes, when waging psychological warfare, three fundamental levels can be distinguished: the strategic level, carried out within the framework of alliances by governments and the highest military commands; the tactical level, which accompanies military operations at the battlefield level; and consolidation operations, conducted among the civilian population in areas under one's own or allied control⁵⁸. This points to a wide range of psychological operations, which is directly linked to the intensity of cognitive war.

In summary, psychological warfare is a key element of cognitive warfare. These are hostile acts involving the use of psychological influence to affect a target group. However, cognitive warfare encompasses a broader context of hostile actions that lead to a change in the way reality is perceived.

⁵⁴ Search term: psychological warfare, *Słownik języka polskiego* (Eng. The Dictionary of the Polish Language), <https://sjp.pwn.pl/slowniki/wojna%20psychologiczna.html> [accessed: 20 XI 2025].

⁵⁵ Search term: psychological warfare, *Wielki słownik języka polskiego* (Eng. The Great Dictionary of the Polish Language), <https://wsjp.pl/haslo/podglad/18679/wojna-psychologiczna> [accessed: 20 XI 2025].

⁵⁶ Search term: psychological warfare, *Encyklopedia Bezpieczeństwa Narodowego* (Eng. Encyclopaedia of National Security), <https://encyklopedia.revite.pl/articles/view/643> [accessed: 20 XI 2025].

⁵⁷ Search term: psychological warfare, *Vademecum Bezpieczeństwa Informacyjnego* (Eng. The Information Security Handbook), <https://vademecumbezpieczenstwainformacyjnego.uken.krakow.pl/2020/03/12/wojna-psychologiczna/> [accessed: 26 XI 2025].

⁵⁸ M. Olechowski, *Wojna psychologiczna – próba zdefiniowania pojęcia* (Eng. Definition of the concept of 'psychological warfare'), "Wiedza Obronna" 2018, wydanie podwójne vol. 262–263, no. 1–2, pp. 91–106. <https://doi.org/10.34752/ahf8-sd31>.

Cognitive warfare

According to the Cyber Defence Forces Component, cognitive warfare (...) is *a war for minds, in which information becomes the key battlefield. Unlike traditional warfare, which focuses on the physical defeat of the enemy, cognitive warfare aims to gain control over people's minds (...)*⁵⁹. During the TEDx Talks, cognitive warfare was described as follows: (...) *cognitive warfare refers to actions designed to shape attitudes and behaviours by influencing or disrupting the cognition (an emotionally charged perception of the world) of a given population, with the aim of gaining an advantage over an adversary and weakening their resilience*⁶⁰. Cognitive warfare involves the use of a wide range of tools, which are often integrated with economic, diplomatic and military activities⁶¹. Niina Meriläinen states that (...) *cognitive warfare has strengthened its place in the strategic, operational and tactical levels of warfare. By targeting cognitive elements such as attitudes, beliefs, and understandings as well as the causal relations these create, cognitive warfare aims to shape the attitudes, beliefs, values, and heritage as well as behaviour of people and compel them to the adversary's aims*⁶². In turn, Agnieszka Szczygielska points out the similarity between cognitive warfare and other forms of warfare: information warfare, cyber warfare and psychological warfare. She claims that (...) *in all these warfares, one can observe various ways of influencing people – their thought processes, their mindset, their sense of security and their understanding of the world. However, cognitive warfare is entirely focused on the human mind, its capabilities and the disruption of cognitive processes*⁶³. The *Journal of Modern Science* also highlighted the characteristics common to many methods of influence and emphasised that cognitive warfare is (...) *a combination of information warfare, intelligence and surveillance as well as reconnaissance, electronic warfare*

⁵⁹ *Dezinformacja* (Eng. Disinformation), <https://www.wojsko-polskie.pl/woc/articles/publikacje-r/dez-informacja/> [accessed: 28 IX 2025].

⁶⁰ A. Karalus, *Czym jest wojna kognitywna?* (Eng. What is cognitive warfare?), YouTube, 28 I 2025, https://www.youtube.com/watch?v=YXIOra_rNGY [accessed: 5 XI 2025].

⁶¹ N. Bugayova, K. Stepanenko, *A Primer on Russian Cognitive Warfare*, https://understandingwar.org/wp-content/uploads/2025/08/ISW20CW20Russian20Cognitive20Warfare2C-20June20302C20202520PDF20FINAL_0.pdf, p. 1 [accessed: 28 IX 2026].

⁶² N. Meriläinen, *Artificial Intelligence as a Tool in Cognitive Warfare on Digital Platforms*, "Proceedings of the 6th International Conference on AI Research, Italy 2025", p. 306. <https://doi.org/10.34190/icair.5.1.4353>.

⁶³ A. Szczygielska, *Wojna kognitywna – źródła i zasadnicze cechy* (Eng. Cognitive warfare – its origins and key characteristics), "Kwartalnik Bellona" 2025, vol. 720, no. 1, pp. 39–40. <https://doi.org/10.5604/01.3001.0055.1652>.

and psychological operations, as well as cyber operations utilising digital and network infrastructure⁶⁴. The scale of the war was also discussed in *Joint Force Quarterly*: (...) in its broadest sense, cognitive warfare is not limited to the military or institutional world (...). It targets the whole of a nation's human capital⁶⁵. Attention was also drawn to the unusual nature of the threats posed by cognitive warfare in *The Defence Horizon Journal*. It was pointed out that, while all forms of war directly or indirectly influence the enemy's will, cognitive warfare should be viewed differently from traditional conceptions. It was emphasised that its impact relates neither to territory nor to dominance over resources, but rather that it is a conflict between different perceptions, beliefs, and even a clash of cultures or civilisations⁶⁶. The North Atlantic Alliance defines cognitive warfare as:

The activities conducted in synchronization with other instruments of power, to affect attitudes and behaviours by influencing, protecting, and/or disrupting individual and group cognitions to gain an advantage. These activities vary greatly, and may encompass supporting or conflicting cultural or personalized components – social psychology, Game Theory, and ethics are all contributing factors⁶⁷.

In summary, cognitive warfare is an integrated psychological operation conducted at the strategic, operational and tactical levels with the aim of influencing the attitudes and behaviour of target groups in order to shape their perception of reality in line with the aggressor's interests and to gain an advantage in all key areas of state functioning.

⁶⁴ A. Skrabacz, A. Pajka, B. Więckowski, *Wojna kognitywna jako nowy wymiar operacji wielodomenowych – mapowanie i profilowanie obszaru badań za pomocą metod bibliometrycznych* (Eng. Cognitive warfare as a new dimension multi-domain operations - mapping and profiling of the research area using bibliometric methods), *Journal of Modern Science* 2025, pp. 711. <https://doi.org/10.13166/jms/203647>.

⁶⁵ M.J. Cheatham et al., *Cognitive Warfare: The Fight for Gray Matter in the Digital Gray Zone*, National Defense University, <https://digitalcommons.ndu.edu/joint-force-quarterly/vol114/iss2/15/> [accessed: 4 XI 2025].

⁶⁶ P.B.M.J. Pijpers, *On Cognitive Warfare: The Anatomy of Disinformation*, *The Defence Horizon Journal*, 21 III 2024, <https://tdhj.org/blog/post/on-cognitive-warfare-the-anatomy-of-disinformation/> [accessed: 26 X 2025].

⁶⁷ *Cognitive Warfare: Strengthening and Defending the Mind*, NATO, 5 IV 2023, <https://www.act.nato.int/article/cognitive-warfare-strengthening-and-defending-the-mind/> [accessed: 15 XI 2025].

Hybrid warfare

Modern conflicts⁶⁸ are addressed using an interdisciplinary approach. According to Hanna Smith, hybrid activities consist of various covert and overt actions, military and/or non-military means, among others, intelligence and cyber operations⁶⁹. This is a combination of (...) *conventional and unconventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors*⁷⁰.

Artur Gruszczyk points out that hybrid warfare comprises elements of: classical and modern warfare, asymmetric conflicts, groundbreaking military technologies and primitive means of influence, struggles over territory and resources, and disputes over identity and values, as well as the confrontation between radicalism and cosmopolitanism⁷¹.

The author of the article proposes defining a hybrid warfare as multidimensional hostile actions combining elements that are kinetic and non-kinetic, regular and irregular, symmetric and asymmetric, conventional and unconventional, which, through the use of information operations and psychological operations, influence the way a target group thinks and acts (Table 1).

⁶⁸ The author deliberately uses the term 'modern' rather than 'contemporary' because, in his view, it is the resources and capacity to wage war that define its nature, and not (merely) the times in which it is waged.

⁶⁹ H. Smith, *Countering Hybrid Threats*, in: *The EU and NATO: The essential partners*, G. Lindstrom, T. Tardy (eds.), Paris 2019, p. 16.

⁷⁰ *Joint Communication to the European Parliament and the Council. Joint Framework on countering hybrid threats – a European Union response*, Brussels, 6.04.2016, JOIN(2016) 18 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52016JC0018> [accessed: 22 X 2025].

⁷¹ A. Gruszczyk, *Hybrydowość współczesnych wojen – analiza krytyczna* (Eng. Hybridity of contemporary wars – a critical analysis), in: *Asymetria i hybrydowość – stare armie wobec nowych konfliktów*, W. Sokała, B. Zapala (sci. eds.), Warszawa 2011, p. 11.

Table 1. Elements of hybrid warfare.

ELEMENTS OF HYBRID WARFARE	
Category	Features and characteristics
Type of damage	<p>kinetic: the use of physical force and destructive power (the actions of personnel and equipment). The desired outcome is the destruction of the enemy's manpower and infrastructure Example: armies destroy one another using soldiers, tanks, aircraft and missile systems, etc.</p>
	<p>non-kinetic: the use of non-kinetic means of engagement in combat, also the so-called <i>soft-power</i>⁷² Example: an enemy carries out information operations, cyber attacks on critical infrastructure, recruits undercover agents</p>
Status of forces and resources	<p>regular: operations carried out by the state's formal, organised and uniformed armed forces. Operations conducted within the framework of international law relating to armed conflicts, which are usually centralised, planned and executed in accordance with established military doctrines Example: two national armies are fighting each other</p>
	<p>irregular: operations carried out by the state's informal, organised forces (e.g. guerrilla forces). They are unevenly distributed across time and space. They are usually employed by smaller forces which have weaker military capabilities Example: guerrillas fighters organise ambushes in the forests and attack ammunition convoys, while the civilian population in the occupied territories organises an uprising against the occupying forces</p>

⁷² *Soft power* is 'a way of influencing others through non-military and non-economic means (...). Attractiveness, image-building, persuading others of one's own views, and, finally, imposing a certain vision or narrative on others (...)', in: A. Rzegocki, *Soft power – niedoceniana siła*, in: *Dylematy strategiczne XXI wieku. Księga jubileuszowa dedykowana profesorowi Michałowi Chorośnickiemu z okazji czterdziestolecia pracy naukowej*, R. Kłosowicz, B. Szlachta, J.J. Węc (sci. eds.), Kraków 2013, p. 158.

ELEMENTS OF HYBRID WARFARE	
Category	Features and characteristics
Comparison of capabilities	<p>symmetric:</p> <p>the warring parties have comparable military capabilities</p> <p>Example: two armies have a similar number of soldiers and a similar amount of equipment, as well as similar technological capabilities and national conditions for waging war</p>
	<p>asymmetric:</p> <p>the warring parties have significantly different military capabilities and also differ markedly in terms of their technological capabilities and the national conditions for waging war. The essence of these measures lies in the use of resources and means that will prove effective in the face of significant differences of the capabilities</p> <p>Example: hackers break into the state's ICT system and bring the country's rail services to a standstill (a small group is fighting the state), a terrorist carries out a bomb attack on the state's infrastructure</p>
Forms and methods	<p>conventional:</p> <p>traditional forms and methods of conducting combat using forces and resources generally intended for that purpose</p> <p>Example: use of rifles, tanks, missiles</p>
	<p>unconventional:</p> <p>non-traditional forms and methods of warfare, utilising forces and resources not intended for the conduct of war</p> <p>Example: use of improvised explosive devices concealed in children's toys, Molotov cocktails, the use of civilian drones for military purposes, Shahid belt⁷³</p>

Source: own elaboration.

In summary, hybrid warfare represents an accumulation of diverse forms, methods and techniques of hostile action: with varying capabilities, across multiple domains and in different environments. It is also a universal concept that enables us to discuss threats that are complex and atypical.

⁷³ Shahid belt – a belt or a vest, filled with explosives and fitted with a detonator, used by suicide bombers. See: search term: Shahid belt, *Wielki słownik języka polskiego*, <https://wsjp.pl/haslo/podglad/85144/pas-szahida> [accessed: 14 XII 2025].

Summary

The author focused on organising and defining the key concepts in the discourse on the hostile use of information within the framework of cognitive warfare in the context of hybrid warfare. He emphasised that viewing the cognitive dimension as a domain of hostile activities leads to the identification of a phenomenon of cognitive warfare, which combines information operations and psychological operations. This warfare is an advanced form of activities that utilise information and psychological influence to gain an advantage on the battlefield. Its aim is to change the attitudes and behaviour of the target group so that they are in line with the aggressor's wishes.

Growing hybrid threats reveal a new dimension to the battle for minds, while the ability to influence perceptions of reality turns the cognitive sphere into a theatre of hostile activities and a significant dimension of contemporary conflicts. The author emphasises that, in view of the growing arsenal of modern technologies, the world will face a new phase of the 'Cold War', which will paralyse the use of kinetic weapons for fear of the destruction of modern civilisations. At that point, a total cognitive war will be waged, the aim of which is to shape people's perception of reality.

Bibliography

Bąkowicz K., *Praktyczne rozumienie dezinformacji wśród polskich przedsiębiorstw: obszary i tendencje* (Eng. Practical understanding of disinformation among Polish enterprises: areas and trends), "Zeszyty Naukowe Akademii Górnośląskiej" 2023, no. 10, pp. 127–137. <https://doi.org/10.53259/2023.10.13>.

Dalinczuk L., *Analiza wywiadowcza jako ważny element bezpieczeństwa narodowego* (Eng. Analysis as an important element of national security), in: *Współczesne zagrożenia bezpieczeństwa państwa cz. II*, Z. Ciekanowski (sci. ed.), Biała Podlaska 2021, pp. 176–183.

Disinformation, in: R. Deacon, *Spyclopedia*, London 1989.

Disinformation, in: R.M. Bennett, *Espionage: An Encyclopedia of Spies and Secrets*, London 2002.

Floridi L., *A Look into the Future Impact of ICT on our Lives*, "The Information Society" 2007, vol. 23, no. 1, pp. 59–64. <https://doi.org/10.1080/01972240601059094>.

Franco C. de, *Media Power and the Transformation of War*, New York 2012.

Frąś J., *Zarządzanie informacją elementem budowy przewagi konkurencyjnej e-przedsiębiorstwa* (Eng. Information management as the key component in creating a competitive edge in e-business), "Studia i Prace Wydziału Nauk Ekonomicznych i Zarządzania" 2011, no. 21, pp. 29–41.

Golitsyn A., *New Lies For Old. The Communist Strategy of Deception And Disinformation*, New York 1984.

Gruszcak A., *Hybrydowość współczesnych wojen – analiza krytyczna* (Eng. Hybridity of contemporary wars – a critical analysis), in: *Asymetria i hybrydowość – stare armie wobec nowych konfliktów*, W. Sokała, B. Zapała (sci. eds.), Warszawa 2011, pp. 9–17.

Kaczmarek K., Karpiuk M., Melchior C., *Disinformation as a Threat to State Security*, "Przegląd Nauk o Obronności" 2024, no. 20, pp. 45–54. <https://doi.org/10.37055/pno/205780>.

Karpiuk W.M., *The Cybersecurity Strategy of the Republic of Poland as a Source of Internal Law*, "Cybersecurity and Law" 2024, no. 2, pp. 234–245.

Kisilowska M., *Przestrzeń informacyjna jako termin informatologiczny* (Eng. Information space as an information science term), "Zagadnienia Informatyki – Studia Informatyczne" 2011, no. 2, pp. 35–52. <https://doi.org/10.36702/zin.666>.

Koncepcja Obronna Rzeczypospolitej Polskiej (Eng. The Defence Concept of the Republic of Poland), Ministerstwo Obrony Narodowej, Warszawa 2017.

Łapszyński A., *Monitoring the Information Environment In the Baltic Sea Region*, "The Baltic Amber. Multinational Corps Northeast Magazine" 2020.

McKnight C., *The Personal Construction of Information Space*, "Journal of the American Society for Information Science" 2000, vol. 51, no. 8, pp. 730–733. [https://doi.org/10.1002/\(SICI\)1097-4571\(2000\)51:8<730::AID-ASI50>3.0.CO;2-8](https://doi.org/10.1002/(SICI)1097-4571(2000)51:8<730::AID-ASI50>3.0.CO;2-8).

Meriläinen N., *Artificial Intelligence as a Tool in Cognitive Warfare on Digital Platforms*, "Proceedings of the 6th International Conference on AI Research", Italy 2025, pp. 306–312. <https://doi.org/10.34190/icaire.5.1.4353>.

Moskalewicz-Kwiatkowska K., *Pasożytnicza strategia rosyjskiej propagandy* (Eng. Parasite strategy of Russian propaganda), Warszawa 2024.

NATO, *Allied Joint Doctrine for Psychological Operations*, AJP-3.10.1(A), 2007, 1-1.

Olechowski M., *Wojna psychologiczna – próba zdefiniowania pojęcia* (Eng. Definition of the concept of 'psychological warfare'), "Wiedza Obronna" 2018, wydanie podwójne vol. 262–263, no. 1–2, pp. 91–106. <https://doi.org/10.34752/ahf8-sd31>.

Otłowski T., *Rosyjskie myślenie o wojnie* (Eng. The Russian perspective on war), “Polska Zbrojna” 2021, no. 5, pp. 80–82.

Pacepa I.M., Rychlak R.J., *Dezinformacja. Były szef wywiadu ujawnia metody dławienia wolności, zwalczania religii i wspierania terroryzmu* (Eng. Disinformation. Former intelligence chief reveals methods used to stifle freedom, suppress religion and support terrorism), Gliwice 2015.

Peplowski A., *Wojna o tajemnice. W tajnej służbie Drugiej Rzeczypospolitej 1918–1944* (Eng. The War for Secrets. The Secret Service of the Second Polish Republic 1918–1944), Kraków 2011.

Romanych M.J., *Visualizing the Information Environment*, “Military Intelligence Professional Bulletin” 2003, vol. 29, no. 3, pp. 5–8.

Rzegocki A., *Soft power – niedoceniana siła* (Eng. Soft power – the underrated power), in: *Dylematy strategiczne XXI wieku. Księga jubileuszowa dedykowana profesorowi Michałowi Chorośnickiemu z okazji czterdziestolecia pracy naukowej*, R. Kłosowicz, B. Szlachta, J.J. Węc (sci. eds.), Kraków 2013, pp. 155–160.

Skrabacz A., Pajka A., Więckowski B., *Wojna kognitywna jako nowy wymiar operacji wielodomenowych – mapowanie i profilowanie obszaru badań za pomocą metod bibliometrycznych* (Eng. Cognitive warfare as a new dimension multi-domain operations - mapping and profiling of the research area using bibliometric methods), “Journal of Modern Science” 2025, pp. 706–722. <https://doi.org/10.13166/jms/203647>.

Smith H., *Countering Hybrid Threats*, in: *The EU and NATO: The essential partners*, G. Lindstrom, T. Tardy (eds.), Paris 2019.

Szczygielska A., *Wojna kognitywna – źródła i zasadnicze cechy* (Eng. Cognitive warfare – its origins and key characteristics), “Kwartalnik Bellona” 2025, vol. 720, no. 1, pp. 27–46. <https://doi.org/10.5604/01.3001.0055.1652>.

Vlahos M., *Entering the Infosphere*, “Journal of International Affairs” 1998, vol. 51, no. 2, pp. 497–525.

Volkoff V., *Psychosocjotechnika. Dezinformacja. Oręż wojny* (Eng. psychosocial engineering. Disinformation. Weapons of war), Warszawa 1991.

Wojnowski M., *Koncepcja „wojny nowej generacji” w ujęciu strategów Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej* (Eng. The concept of ‘modern warfare’ formulated by strategists of the Russian Federation Armed Forces Headquarters), “Przegląd Bezpieczeństwa Wewnętrznego” 2015, no. 13, pp. 13–39.

Z tarczą! Jak chronić się przed dezinformacją? (Eng. With a shield! How can you protect yourself from disinformation?), K. Mikulski, M. Krawczyk (eds.), Kraków 2021.

Zielonka Z., Rumiński K., *Poland Place of Freedom*, Ministerstwo Obrony Narodowej, Warszawa 2017.

Internet sources

Balcewicz J., *Zwalczanie dezinformacji w internecie: podejście europejskie* (Eng. Combating disinformation online: European approach), 26 IV 2018, <https://cyberpolicy.nask.pl/zwalczanie-dezinformacji-w-internecie-podejscie-europejskie> [accessed: 17 X 2025].

Biuro Bezpieczeństwa Narodowego 2015–2025 (Eng. National Security Bureau 2015–2025), https://www.bbn.gov.pl/pl/informacje-o-bbn/publikacje/10209_Biuro-Bezpieczenstwa-Narodowego-2015-2025.html [accessed: 28 IX 2026].

Borden A., *What Is Information Warfare?*, <https://www.airuniversity.af.edu/Portals/10/ASP/journals/Chronicles/borden.pdf> [accessed: 20 V 2024].

Bugayova N., Stepanenko K., *A Primer on Russian Cognitive Warfare*, https://understandingwar.org/wp-content/uploads/2025/08/ISW20CW20Russian20Cognitive20Warfare2C-20June20302C20202520PDF20FINAL_0.pdf [accessed: 28 IX 2026].

Calkayis M., *Contemporary Information Warfare, Artificial Intelligence, and Challenges for Democracies*, NAVI, 26 X 2025, <https://nato-veterans.org/contemporary-information-warfare-artificial-intelligence-and-challenges-for-democracies/> [accessed: 6 XI 2025].

Cheatham M.J., Geyer A.M., Nohle A.P., Vazquez J.E., *Cognitive Warfare: The Fight for Gray Matter in the Digital Gray Zone*, National Defense University, <https://digitalcommons.ndu.edu/joint-force-quarterly/vol114/iss2/15/> [accessed: 4 XI 2025].

Chroń się przed dezinformacją (Eng. Defend yourself against disinformation), NASK, <https://www.nask.pl/instytut/dla-ciebie/dezinfo> [accessed: 19 IX 2025].

Cognitive Warfare: Strengthening and Defending the Mind, NATO, 5 IV 2023, <https://www.act.nato.int/article/cognitive-warfare-strengthening-and-defending-the-mind/> [accessed: 15 XI 2025].

Counter-FIMI Toolbox for Diplomats. A Conceptual Framework, <https://community-democracies.org/app/uploads/2025/01/Counter-FIMI-Toolbox.pdf> [accessed: 2 IX 2026].

Creation of the European External Action Service, European Union External Action, 19 VIII 2021, https://www.eeas.europa.eu/eeas/creation-european-external-action-service_en [accessed: 20 XII 2025].

Czy wiesz jak chronić się przed dezinformacją? (Eng. Do you know how to defend yourself against disinformation?), Komenda Powiatowa Policji w Oławie, 24 XI 2024, <https://olawa.policja.gov.pl/doa/aktualnosci/bieza/132251,Czy-wiesz-jak-chronic-sie-przed-dezinformacja.html> [accessed: 15 IX 2025].

Disinformation affecting the EU: tackled but not tamed. Special report, https://www.eca.europa.eu/Lists/ECADocuments/SR21_09/SR_Disinformation_EN.pdf [accessed: 15 X 2025].

Disinformation: 10 steps to protect yourself and others, European Parliament, 11 VI 2025, <https://www.europarl.europa.eu/topics/en/article/20250603STO28720/disinformation-10-steps-to-protect-yourself-and-others> [accessed: 21 X 2025].

Dezinformacja (Eng. Disinformation), <https://www.wojsko-polskie.pl/woc/articles/publikacje-r/dezinformacja/> [accessed: 28 IX 2025].

Dlaczego obca propaganda jest skuteczna w obszarze obronności? (Eng. Why is foreign propaganda effective in the field of defence?), Stop Fake Org, 5 VIII 2019, <https://www.stopfake.org/pl/dlaczego-obca-propaganda-jest-skuteczna-w-obszarze-obronnosci/> [accessed: 29 X 2025].

Encyklopedia Bezpieczeństwa (Eng. Encyclopaedia of security), vol. 5, O. Wasiuta, S. Wasiuta (eds.), <https://inob.uken.krakow.pl/wp-content/uploads/sites/37/2023/10/Encyklopedia-tom-5.pdf> [accessed: 2 XII 2025].

Encyklopedia Bezpieczeństwa Narodowego, Encyklopedia Bezpieczeństwa (Eng. Encyclopaedia of National Security, Encyclopaedia of Security), vol. 5, O. Wasiuta, S. Wasiuta (eds.), <https://encyklopedia.revite.pl/articles/view/643> [accessed: 20 XI 2025].

Gorzelnik N., *Twój post na fejsie może kosztować życie. Oto jak wrogie wywiady wykorzystują social media* (Eng. Your Facebook post could cost someone their life. Here's how hostile intelligence services exploit social media), INN Poland, 28 III 2022, <https://innpoland.pl/177769,jak-twoje-dzialania-w-sieci-wspieraja-rosyjski-wywiad> [accessed: 28 VIII 2024].

Karalus A., *Czym jest wojna kognitywna?* (Eng. What is cognitive warfare?), YouTube, 28 I 2025, https://www.youtube.com/watch?v=YXIOra_rNGY [accessed: 5 XI 2025].

NATO 2022 Strategic Concept, NATO, 29 VII 2022, <https://www.nato.int/en/about-us/official-texts-and-resources/strategic-concepts/nato-2022-strategic-concept> [accessed: 9 XII 2024].

Nogacki R., Surdyk K., *Teoria i praktyka działań dezinformacyjnych* (Eng. The theory and practice of disinformation campaigns), Profesjonalny Wywiad Gospodarczy Skarbiec, 19 II 2020, <https://www.wywiad-gospodarczy.pl/teoria-i-praktyka-dzialan-dezinformacyjnych.html> [accessed: 19 VIII 2025].

Oleksiejuk M., *Dangerous Russian Siege Mentality*, Warsaw Institute, 31 VIII 2020, <https://warsawinstitute.org/dangerous-russian-siege-mentality/> [accessed: 29 VIII 2025].

Pijpers P.B.M.J., *On Cognitive Warfare: The Anatomy of Disinformation*, The Defence Horizon Journal, 21 III 2024, <https://tdhj.org/blog/post/on-cognitive-warfare-the-anatomy-of-disinformation/> [accessed: 26 X 2025].

Protecting the Alliance Against the Threat of Cognitive Warfare, YouTube, 9 V 2023, <https://www.youtube.com/watch?v=4Pn57uoyYEA> [accessed: 5 XI 2025].

Rozpoznawanie nieprawdziwych informacji (Eng. Identifying false information), Serwis Rzeczypospolitej Polskiej, <https://www.gov.pl/web/baza-wiedzy/roznawanie-nieprawdziwych-informacji> [accessed: 20 III 2023].

Słownik języka polskiego (Eng. The Dictionary of the Polish Language), <https://sjp.pwn.pl/sjp/manipulacja;2481186> [accessed: 10 IX 2025].

Słownik języka polskiego (Eng. The Dictionary of the Polish Language), <https://sjp.pwn.pl/slowniki/wojna%20psychologiczna.html> [accessed: 20 XI 2025]

Tomala L., *Kto wierzy w fake newsy? Badacze chcą zwalczać szkodliwe informacje jak epidemie* (Eng. Who believes in fake news? Researchers want to combat harmful information as if it were an epidemic), *Nauka w Polsce*, 7 II 2021, <https://naukawpolsce.pl/aktualnosci/news%2C86178%2Ckto-wierzy-w-fake-newsy-badacze-chca-zwalczac-szkodliwe-informacje-jak> [accessed: 15 X 2025].

Tzu S., *The Art of War*, https://ebook-mecca.com/online/The_Art_of_War.pdf [accessed: 27 IX 2025].

Vademecum Bezpieczeństwa Informacyjnego (Eng. The Information Security Handbook), <https://vademecumbezpieczenstwainformacyjnego.uken.krakow.pl/2020/03/12/wojna-psychologiczna/> [accessed: 26 XI 2025].

Wielki słownik języka polskiego (Eng. The Great Dictionary of the Polish Language), <https://wsjp.pl/haslo/podglad/18679/wojna-psychologiczna> [accessed: 20 XI 2025].

Wielki słownik języka polskiego (Eng. The Great Dictionary of the Polish Language), <https://wsjp.pl/haslo/podglad/85144/pas-szahida> [accessed: 14 XII 2025].

Wykorzystanie sztucznej inteligencji w wykrywaniu dezinformacji w Internecie (Eng. The use of artificial intelligence in detecting disinformation on the internet), Serwis Rzeczypospolitej Polskiej, 10 VIII 2023, <https://www.gov.pl/web/5g/wykorzystanie-sztucznej-inteligencji-w-wykrywaniu-dezinformacji-w-internecie> [accessed: 27 X 2025].

Other documents

Recommendations of the Committee of Ministers to member states on the remit of public service media in the information society (Adopted by the Committee of Ministers on 31 January 2007 at the 985th meeting of the Ministers' Deputies), CM/Rec (2007)3, <https://search.coe.int/cm?i=09000016805d6bc5> [accessed: 14 IX 2025].

Joint Communication to the European Parliament and the Council. Joint Framework on countering hybrid threats – a European Union response, Brussels, 6.04.2016, JOIN(2016) 18 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52016JC0018> [accessed: 22 X 2025].

Col. Tomasz Gergelewicz, PhD

Doctor of sciences in the discipline of security sciences. He researches the impact of information operations on security and works on building societal resilience to cognitive threats in practice. He gained experience in the field of strategic communication and countering disinformation at the Operational Centre of the Minister of National Defence and at the Academic Centre for Strategic Communication at the War Studies University. He carries out his teaching and journalistic work in the field of security strategy, strategic communication and countering hostile information operations, including the use of technologies based on artificial intelligence.

Contact: t.gergelewicz@wp.pl