Marek Przybyła, MA
University and MA in Logistics from the Military University of Technology
marek_przybyła@yahoo.com
ORCID: 0009-0007-0044-4495

DOI: 10.26410/SF_2/25/8

COUNTERING DISINFORMATION AS AN ELEMENT OF COMBATING CYBER THREATS AGAINST THE REPUBLIC OF POLAND

Abstract

The aim of this paper is to characterise the phenomenon of disinformation as one of the primary cyber threats undermining the security system of the Republic of Poland. Ensuring information security and cybersecurity is among the strategic priorities of the European Union. Disinformation constitutes a key instrument in hybrid operations, which are particularly prominent today, especially in the context of Russian activity. The near-revolutionary pace of technological advancement has enabled the Russian Federation to refine its disinformation campaigns, prompting the European Union, among others, to take action to counter this phenomenon. The main objective of the author is to present academically grounded benefits resulting from the development of effective methods to combat disinformation–regarded as one of the most urgent and significant challenges to Poland's information security. The solutions proposed in this publication may serve as a point of departure for further analysis, decision-making, legislative amendments, or the drafting of additional reports in this area. The paper relies on theoretical research methods. The reflections presented suggest that combating cyber threats requires the development of a system composed of effective processes to counter such risks–processes that, in turn, necessitate cooperation between state and private entities as well as society at large. The conclusions drawn may contribute to reducing the level of risk and enhancing the level of information security in the Republic of Poland.

Keywords

Cybersecurity, disinformation, fake news, fact-checking, microtargeting

Introduction

A fundamental component of the functioning of a state's overall security system is the identification of all types of threats, including cyber threats, which may pose risks, among others, to individuals holding senior positions within the government[1]. It is difficult nowadays to dispute the assertion that "cybersecurity is of vital importance not only to national prosperity and security, but also to the very functioning of our democracy, our freedoms, and our values[2]. The "National Security Strategy of the Republic of Poland", published in 2020, indicates that the neo-imperial policy of the Russian Federation undermines the foundations of the European security system. Russia pursues its objectives without resorting to military force by engaging in sub-threshold activities (hybrid operations[3]) through non-military means. With reference to cyberspace[4] and the information space, these include, among others, cyberattacks, disinformation, and manipulation[5]. It is not only Ukraine[6], that has fallen victim to Russian hybrid operations conducted in cyberspace, but also the Euro-Atlantic community. Hybrid operations in cyberspace involve planned and coordinated actions combining various forms of pressure, carried out either through a state's own resources or with the involvement of external actors, such as politically motivated hacktivists[7] (often referred to as cyber warriors), as well as through the exploitation of national, ethnic, or religious minorities. Hybrid activities in cyberspace typically include the simultaneous execution of disinformation campaigns and unconventional attacks within the information space. The activity of so-called cyber armies typically emerges during armed conflicts and international crises[8].

1 T. Goryca, *Selected Operational and Intelligence Activities as Elements of Bodies*, *Security Forum*, no. 1, 2024, WSB Academy Press, Dąbrowa Górnicza, p. 58.

2 Proposal for a Regulation of the European Parliament and of the Council on ENISA, repealing Regulation (EU) No 526/2013, and on cybersecurity certification in the field of information and communication technologies (OJ EU C 227/13 of 28.6.2018).

3 The underlying assumption of Russia's hybrid warfare is the weakening of the adversary's defensive potential – a form of so-called sub-threshold aggression carried out during an official state of peace through sabotage and information operations. Source: M. Wojnowski, *Mit „wojny hybrydowej". Konflikt na terenie państwa ukraińskiego w świetle rosyjskiej myśli wojskowej XIX–XXI wieku*, [in:] *Przegląd Bezpieczeństwa Wewnętrznego. Wojna hybrydowa – Wydanie Specjalne*, Wydawnictwo Agencji Bezpieczeństwa Wewnętrznego, Wiązowna 2015, no. 15, p. 23.

4 Cyberspace is understood as a virtual domain for the processing and exchange of information, formed by ICT systems, within which interactions occur between networks and users.

5 *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2020, pp. 6–8.*

6 See more in: S. Tomaszewski, *Media elektroniczne jako instrument walki informacyjnej*, [in:] W. Fehler (ed.), *Informacyjny Wymiar Bezpieczeństwa Państw i Jednostek*, Wydawnictwo Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach, Siedlce 2021, p. 240.

7 A term derived from the combination of two words: hacker and activist.

8 T. Nowak, *Działania hybrydowe w cyberprzestrzeni prowadzone przez Rosję jako zagrożenie dla bezpieczeństwa euroatlantyckiego*, [w:] M. Banasik, A. Rogozińska (red.), *Zagrożenia Federacji Rosyjskiej i Bezpieczeństwo Międzynarodowe*, Wydawnictwo Difin SA, Warszawa 2020, s. 73.

Methodology

The central problem addressed in this article is expressed in the form of the following research question: How can disinformation be effectively and efficiently countered in the process of combating cyber threats against the Republic of Poland?

During the research process, theoretical research methods were employed, including: analysis (which enabled the identification of individual components and distinctive features of the subject under study), synthesis (which allowed for the establishment of relationships between the various elements of the subject), definition (which facilitated the clarification of terms related to the research topic), and inference (which supported the formulation of new conclusions concerning the subject under investigation)[9].

The analysis was based on the available literature related to the subject of the research[10], In particular, the analysis encompassed Polish and foreign-language monographs, printed academic articles, online sources, as well as specialised textbooks, manuals, guidelines, and applicable legal regulations.

Disinformation as a Contemporary Form of Cyber Threat

According to T. Nowak, the most significant tools employed by Russia against Euro-Atlantic countries between 2014 and 2019 included: disinformation [11], manipulation [12], fake news[13], information disruption, cyberattacks, and cyberespionage[14]. Disinformation campaigns constitute a crucial component of hybrid operations conducted in cyberspace. By employing manipulation, the Russian Federation constructs a negative image of the authorities and societies of targeted states, while also undermining the reputation of their armed forces. To this end, among other methods, highly impactful fake news is generated. At the end of December 2019, a fake

9 See more in: *Bezpieczeństwo. Teoria–Badania–Praktyka*, A. Czupryński, B. Wiśniewski, J. Zboina (scientific eds.), Centrum Naukowo-Badawcze Ochrony Przeciwpożarowej im. Józefa Tuliszkowskiego – Państwowy Instytut Badawczy, Józefów 2015, p. 32.

10 See more in: *Nauki o bezpieczeństwie. Wybrane problemy badań*, A. Czupryński, B. Wiśniewski, J. Zboina (scientific eds.), Centrum Naukowo-Badawcze Ochrony Przeciwpożarowej im. Józefa Tuliszkowskiego – Państwowy Instytut Badawczy, Józefów 2017.

11 In the traditional sense, disinformation refers to false information that has been deliberately and intentionally fabricated, as well as to planned actions involving the transmission of untrue content to an adversary. The objective of disinformation efforts is to influence the decision-making processes of another state's authorities. Such activities may be carried out through mass media or by means of operational measures undertaken by intelligence services. Source: P. Bączek, *Dezinformacja jako zagrożenie dla bezpieczeństwa informacyjnego współczesnych społeczeństw*, *Security Review*, Wydawnictwo Instytut Analizy Ryzyka Sp. z o.o., Rzeszów 2020, no. 4 (17), pp. 9–11.

12 Most broadly, manipulation can be defined as "any covert, intentional, and deliberate influence exerted on recipients in order to affect their attitudes and, ultimately, their behaviour." Source: M. Golka, *Bariery w komunikowaniu i społeczeństwo (dez)informacyjne*, Wydawnictwo Naukowe PWN, Warszawa 2008, p. 112.

13 Fake news can be defined as "information intended to deliberately and knowingly mislead the recipient in order to gain image-related, financial, psychological, propaganda, political, or economic benefits." Source: B. Rejman, K. Rejman, *Fake news jako narzędzie działań dezinformacyjnych a bezpieczeństwo współczesnych systemów społeczno–ekonomicznych*, [in:] K. Rejman, M. Wilczyńska, J. Wołejszo (eds.), *Bezpieczeństwo Informacji Wobec Współczesnych Zagrożeń*, Wydawnictwo Kaliskie Towarzystwo Przyjaciół Nauk, Kalisz 2023, p. 216.

14 T. Nowak, *Działania hybrydowe w cyberprzestrzeni…*, op. cit., p. 74.

news story was disseminated via bots, reproducing an article from *Russia Today* which claimed that Poland had attempted to pressure Belarus into abandoning its cooperation with Russia and moving closer to NATO. The authors of the manipulated information exploited the widely known view that the eastward expansion of NATO infrastructure poses a military threat to Russia[15]. Moreover, during the peak of military operations in the Donbas region, Facebook posts were published targeting residents of western Ukraine, encouraging them to leave the country for economic reasons, with Poland being the primary destination. Additionally, these posts stirred anti-government sentiment among the population of Lviv by recalling that Lviv was once a Polish city. Other content included links to external websites about visa-free travel between Ukraine and EU member states, as well as information on how to find employment in Poland[16]. Among the most significant consequences of Russian hybrid activities in cyberspace are: the discrediting of EU and NATO member states; the fuelling of antagonisms rooted in historical experiences; efforts to sow division and obstruct cooperation and decision-making processes; and the consolidation of pro-Russian groups within the target countries[17].

Ensuring information security, ICT security (cybersecurity), and operational[18] continuity is one of the strategic priorities of the European Union.

To this end, in 2015, an action plan was established in response to Russian disinformation. As a result, a working group called the *East StratCom Task Force* (ESTF) was created. The ESTF consists of a team of analysts and experts who monitor the course of pro-Russian disinformation campaigns[19]. There is a visible trend indicating that Brussels is strengthening its capabilities in identifying and countering disinformation. Efforts have been undertaken to build structures aimed at enhancing situational awareness and supporting decision-making processes.

Since 2014, there has been a significant increase in offensive activity in cyberspace carried out by entities that are either part of Russian state structures or act on their behalf or in their interest, conducting large-scale disinformation campaigns primarily targeting NATO and EU member states. It is worth noting that this phenomenon is not limited to the Russian context. Similar actions are undertaken by other international actors aspiring to global or regional power status. Well-documented examples include China (Karásková 2020) and Iran (Kasapoglu 2020). It should be

15 T. Nowak, *Działania hybrydowe w cyberprzestrzeni…*, op. cit., pp. 78–79.

16 R. DiResta, S. Grossman, *Potemkin Pages & Personas: Assessing GRU Online Operations, 2014–2019*, ed. Stanford Cyber Policy Center, Stanford 2019, pp. 54–56.

17 T. Nowak, *Działania hybrydowe w cyberprzestrzeni…*, op. cit., p. 83.

18 Szerzej, T. Goryca, *Risk and threats in protective measures of the units responsible for security of executive states bodies*, „Security Forum" 2022, nr 1, Wydawnictwo Akademia WSB, Dąbrowa Górnicza 2022.

19 T. Nowak, *Polityka Unii Europejskiej w latach 2014-2019 wobec działań hybrydowych Federacji Rosyjskiej*, [w:] M. Banasik, A. Rogozińska (red.), *Zagrożenia Federacji Rosyjskiej i Bezpieczeństwo Międzynarodowe*, Wydawnictwo Difin SA, Warszawa 2020, s. 135. See more in: T. Goryca, Risk and Threats in Protective Measures of the Units Responsible for Security of Executive State Bodies, Security Forum 2022, no. 1, Wydawnictwo Akademia WSB, Dąbrowa Górnicza 2022. T. Nowak, Polityka Unii Europejskiej w latach 2014–2019 wobec działań hybrydowych Federacji Rosyjskiej, [in:] M. Banasik, A. Rogozińska (eds.), Zagrożenia Federacji Rosyjskiej i Bezpieczeństwo Międzynarodowe, Wydawnictwo Difin SA, Warszawa 2020, p. 135.

emphasised that tools of informational influence and modern channels of information dissemination are used–albeit to varying degrees–by virtually all states across the world[20]. Admittedly, not all states engage in disinformation activities or employ fabricated information sequences. Moreover, information warfare is not exclusively the domain of state actors. Non-state entities are also active in this area–including terrorist organisations such as Daesh (ISIS) (Winter 2019)[21].

The development of effective methods for combating disinformation has become one of the most urgent and significant challenges facing contemporary science. At the same time, it is an exceptionally interdisciplinary issue, requiring intensive collaboration across the natural sciences, medical sciences, social sciences, and the humanities[22].

Countering Disinformation

In developing a framework for countering disinformation in Poland, it is essential to examine the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions – *Tackling online disinformation: a European approach* (April 2018), which outlines four fundamental pillars for combating disinformation on the Internet[23]:

- improving transparency regarding the origin of content and the means by which it is financed;
- promoting information diversity in order to foster users' critical thinking and support high-quality journalism;
- strengthening the credibility of information by indicating whether it can be trusted;
- developing coordinated actions involving broad engagement of public authorities, online platforms, advertisers, trusted fact-checking entities, journalists, and media groups[24].

---

20 There is a widely held view that AI (AI – an acronym formed from the initial letters of the term "artificial intelligence") will enable states, corporations, and organisations to spread false content more effectively–content that will appear credible. As a result, the problem of disinformation dissemination will become even more difficult to resolve. Source: P. Bączek, Wyzwania i zagrożenia dezinformacyjne w kontekście rozwoju sztucznej inteligencji, [in:] W. Fehler (ed.), Informacyjny Wymiar Bezpieczeństwa Państw i Jednostek, Wydawnictwo Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach, Siedlce 2021, p. 136.

21 R. Kupiecki, F. Bryjka, T. Chłoń, *Dezinformacja międzynarodowa – Pojęcie, Rozpoznanie, Przeciwdziałanie*, Wydawnictwo Naukowe Scholar, Warszawa 2022, p. 22.

22 J. Kuś, *Zjawisko dezinformacji z perspektywy psychologicznej: uwarunkowania i przeciwdziałanie*, [in:] K. Stasiuk-Krajewska, M. Wenzel (eds.), *Dezinformacja w czasach kryzysu*, Wydawnictwo Adam Marszałek, Toruń 2024, p. 77.

23 M. Danek, *Modele walki z dezinformacją: od restrykcji do współpracy*, [in:] M. Bernaczyk, T. Gąsior, J. Misiuna, M. Serowaniec (eds.), *Znaczenie nowych technologii dla jakości systemu politycznego – ujęcie politologiczne, prawne i socjologiczne*, Wydawnictwo Naukowe Uniwersytetu Mikołaja Kopernika, Toruń 2020, p. 143.

24 The media play a key role in shaping how we perceive the world around us. For many people, the Internet has become the primary tool for acquiring knowledge about the world, a natural environment for gaining experience and fulfilling social needs, as well as a means of effective communication and access to information on an unprecedented scale. Source: See M. Szulc, Manipulowanie informacją w sieci za pomocą fake newsów jako zagrożenie dla młodzieży, [in:] Psychologia Wychowawcza, Wydawnictwo Uniwersytet Gdański, Gdańsk 2020, vol. 599730, no. 17, pp. 140–157.

Moreover, the budget of the European External Action Service for combating disinformation was increased from €1.9 million to €5 million, and a *Rapid Alert System* was established. Co-developed by national contact points, this system enables real-time alerts regarding foreign disinformation campaigns[25]. On 14 June 2019, the European Commission published a report on the implementation of its action plan against disinformation. The report emphasised that significant progress had been made in identifying and countering disinformation, cooperating with online platforms, raising public awareness, and ensuring a relatively calm and secure conduct of the European elections[26]. Nevertheless, the problem of disinformation has not disappeared, and disinformation campaigns remain highly effective[27].

On 16 June 2022, the European Commission presented an enhanced Code of Practice on Disinformation, linked to the Digital Services Act, stating that disinformation has become a very serious threat capable of significantly impacting the political and social situation worldwide[28]. In recent years, there have been large-scale disinformation attempts, typically associated with major geopolitical events such as Russia's invasion of Ukraine in 2022 or the U.S. elections in 2016 and 2020. As early as 2016, it was demonstrated that disinformation accounted for over 70% of all circulated content in social media spaces. Moreover, it has been observed that disinformation can significantly suppress the potential for social innovation, which in turn may lead to a decline in a state's economic capacity[29].

In order to combat disinformation, it is essential to undertake systemic action within the broadly understood sphere of education. Such efforts must encompass all levels of the educational system–primary, secondary, and higher education. It would also be advisable to implement similar initiatives targeting older individuals, for instance those participating in lifelong learning programmes such as universities of the third age. a particularly important role in exposing fake news is played by media professionals, as well as members of the academic and expert communities. The responsibility of supporting the state in countering this phenomenon rests largely on their shoulders. It is worth considering whether cooperation should be established between state institutions and other entities responsible for education, with the aim of building infrastructure to fight fake news. It is also crucial to implement mechanisms that enable the rapid verification of potentially false information. Such analysis should take place at an expert level and be widely disseminated among the public. This practice is referred to as *fact-checking*. Fact-checking organisations are

25 M. Danek, *Modele walki z dezinformacją…*, op. cit., p. 144.

26 Tamże, s. 145.

27 The power of its dissemination is attributed to the rapid pace of technological advancement, widespread access to information, the speed at which it spreads, and its specific digital features such as editability, openness, interactivity, and high shareability. Source: K. Stasiuk-Krajewska, *Dezinformacja. Próba ujęcia dyskursywnego*, *Media – Kultura – Biznes*, Wydawnictwo Uniwersytet Gdański, Gdańsk 2023, vol. 1 (14), p. 56.

28 Such activity is less costly than conventional military confrontation, yet equally severe in terms of its consequences. Source: K. Janik, *Państwo, Polityka, Bezpieczeństwo Wewnętrzne*, Wydawnictwo Adam Marszałek, Toruń 2021, p. 57.

29 M. Danek, *Modele walki z dezinformacją…*, op. cit., s. 59.

institutions, associations, or groups of individual experts whose primary task is to verify the accuracy of public claims and information (e.g., the association *Demagog*). These organisations most commonly operate as part of newsrooms or as independent non-governmental organisations, and less frequently within academic institutions.

Fact-checking, understood as the professional verification of the authenticity of facts and information circulating in the media space, has become the most widespread method of combating disinformation. By definition, it is a process involving the assessment of the truthfulness of content conveyed in written and spoken messages that enter the public sphere and have been formulated within a specific context[30].

The most active fact-checking organisation is the *International Fact-Checking Network* (IFCN). Its main goal is to bring together individuals and institutions involved in combating disinformation and verifying facts, by facilitating networking, building collaborative frameworks through advocacy, organising various events, training sessions, conferences, expert meetings, and by providing financial support to entities engaged in fact-checking activities.

It is also worth examining the FactcheckEU project, which was initiated by 19 fact-checking entities from 13 countries with the aim of verifying information during the European Parliament elections. Another noteworthy initiative is the SOMA project (Social Observatory for Disinformation and Social Media Analysis) – launched by the European Commission in cooperation with five fact-checking organisations from Greece, Italy, and Denmark. Its objective is to promote campaigns aimed at combating disinformation and to organise training programmes for experts. The relevance of fact-checking organisations is evidenced by the fact that, in the first six weeks of the Russia–Ukraine conflict in 2022 alone, nearly 20,000 reports of disinformation were submitted through just one fact-checking project. Moreover, from the outbreak of the war until 31 August 2023, over 15 billion mentions related to Russian disinformation were recorded.

Educational efforts aimed at combating disinformation should also include media literacy education[31]. The primary normative act of the European Union concerning media education is the Audiovisual Media Services Directive (AVMSD) of 2018. It assigns responsibilities to various media market stakeholders in promoting and developing media literacy. It also obliges EU Member States to support the development of media-related competencies and implement appropriate measures in this regard, as well as to submit regular reports to the European Commission. For instance, France

30 M. Kowalska-Chrzanowska, P. Krysiński, N. Pamuła, *Metody i narzędzia budowania społecznej odporności na dezinformację: od fact-checkingu po edukację medialną*, Wydawnictwo Naukowe Uniwersytetu Mikołaja Kopernika, Toruń 2024, p. 72.

31 Researchers are divided on the issue of disinformation. Some perceive it as occurring exclusively on social media platforms, while others point to its presence in more traditional forms of mass communication–such as television, radio, and the press–as well as in private life and the political sphere. Sources: A. Khan, K. Brohman, S. Addas, *The Anatomy of "Fake News": Studying False Messages as Digital Objects*, *Journal of Information Technology*, ed. Sage, 2022, vol. 37, iss. 2, pp. 122–143; and *The Disinformation Age: Politics, Technology and Disruptive Communication in the United States*, eds. W. L. Bennet, S. Livingston, Cambridge University Press, Cambridge 2021, p. 28.

introduced the Act on Combating the Manipulation of Information of 22 December 2018, which imposes on internet platforms under French jurisdiction the obligation to fight the spread of false information, including through initiatives promoting media and information literacy[32]. In 2022, Italy launched a national centre for combating disinformation – the Italian Digital Media Observatory (IDMO) at Luiss Guido Carli University (LUISS), which forms part of a European network established at the initiative of eight Member States. The project is funded by the EU budget[33].

Poland lacks a coherent strategy regarding media literacy and the use of new media by young people. Nevertheless, the issue has received attention within the programmes of the Ministry of Education and Science and the Ministry of Digital Affairs. Media literacy education was introduced in 1999 in primary and lower secondary schools; however, the implementation of the programme proved inconsistent, and the media education curriculum was abandoned in 2008[34]. It is worth examining selected initiatives that support the fight against disinformation in Poland and worldwide: Akademia Fact-Checkingu, Demagog Educational Platform, #FakeHunter EDU, CovidHub EDU, MedFake, EUvsDisinfo, and Fake News & Elders.

NATO experts recommend that mass media analyse information and verify facts prior to publication or further dissemination, and educate the public about disinformation activities in online media by providing analyses and studies of various disinformation tactics and manipulation techniques. Government institutions, in turn, are advised to identify and expose sources of disinformation, which entails placing greater emphasis on analysing the information environment. Ultimately, this leads to faster identification of disinformation activities and their impact on public discourse[35].

At the individual level, actions should be taken that allow for at least partial differentiation between true and false content. The method by which the credibility of information can be verified is based on four fundamental elements: assessing the source, the fact, the image, and the timeliness. The International Federation of Library Associations and Institutions (IFLA) recommends eight key steps for verifying fake news:

- Check the source – the website's data, editorial details, domain ownership, and sources of funding;
- Check the authors – their actual identity, qualifications, and professional background;
- Check the date – the relevance and timeliness of the topic in relation to real-world events;
- Read beyond – do not rely solely on headlines;
- Consult additional sources of information;

32 M. Kowalska-Chrzanowska, P. Krysiński, N. Pamuła, *Metody i narzędzia budowania…*, op. cit., p. 100.
33 Ibid, p. 188.
34 Ibid, p. 145-146.
35 Ibid, p. 67.

- Avoid bias and refrain from judging based on personal prejudices;
- Determine whether it may be satire or a joke by checking other sources;
- Ask the experts – confront questionable claims and information by consulting professionals in the relevant field[36].

While the above recommendations cannot fully immunise individuals and groups against disinformation, efforts to combat disinformation should involve not only government institutions, security services, and organisations, but also individual citizens.

It is also worth noting the GANESA[37], programme, funded by the European Parliament, under which teaching scenarios were developed – including lesson plans, workshops, and seminar formats. The above are components of an educational process aimed at shaping attitudes in the younger generation that are desirable in a civic society, as well as supporting conscious, responsible, and well-informed decision-making in personal life. An example lesson plan has been proposed for upper secondary school students, focusing on counteracting disinformation. The primary objective of the class is to develop students' awareness of what fake news is and how to distinguish it from true information. An additional goal is to teach students the following mechanisms:

- verification of information in the media;
- critical selection of sources;
- distinguishing between the concepts of: manipulation, disinformation, post-truth, stereotype, information bubble, and virality[38];
- identifying the above phenomena in texts[39].

Moreover, a procedure for verifying information has been proposed:

- checking the source from which the information originates;
- reading the full content of the article rather than relying solely on the headline;
- checking who the author of the text is;
- paying attention to footnotes and annotations;
- analysing any accompanying images for signs of photomontage or manipulation;
- ensuring that the information being verified is not a joke or satire;
- thinking three times before sharing the information[40].

Well-developed fact-checking projects and effective efforts in the field of media education constitute essential components of the disinformation counteraction system. To this end, broad cooperation should be established between state institutions and other entities responsible for education, in order to build infrastructure for combating disinformation.

36 M. Kowalska-Chrzanowska, P. Krysiński, N. Pamuła, *Metody i narzędzia…*, op. cit., p. 64.

37 www.ganesa.uni.wroc.pl, [accessed 6 May 2025].

38 The tendency for an image, video, or piece of information to spread rapidly and widely from one internet user to another.

39 *Dialog w Unii Europejskiej – scenariusze zajęć dydaktycznych z zakresu…*, op. cit., s.103.

40 Tamże, s. 105.

Pitfalls in Combating Disinformation

The European Union defines disinformation as verifiably false or misleading information that is created, presented, and disseminated for economic gain or to intentionally deceive the public, and which may cause public harm. In relation to this definition, among the indicators that fall under the category of "public harm" are "threats to democratic political processes." One such threat is undoubtedly political advertising, which in recent years has been increasingly tailored to specific target audiences–meaning it is precisely targeted. The practice of targeting and microtargeting–i.e. directing messages at narrowly defined audience segments–originates from the advertising sector and involves adjusting the message to the specific needs of recipients. The use of microtargeting techniques during the U.S.[41] presidential campaign and the referendum that led to the United Kingdom's withdrawal from the European Union demonstrates that, in the political sphere, this practice can have serious consequences for public life. Microtargeting remains a phenomenon that has not yet been thoroughly studied in the context of Polish politics; however, it is becoming increasingly common due to the growing use of new technologies by politicians, which make such practices possible[42]. The Code of Practice developed by the European Commission includes a commitment requiring online platform operators to ensure that information concerning targeting and microtargeting is publicly accessible, and that users can find out why a given advertisement–including political advertising–is being directed specifically at them[43]. It is worth emphasising that the Polish legislator has not yet introduced any measure requiring the public disclosure of information regarding the targeting and microtargeting of political advertisements.

There are instances in which the fight against fake news takes the form of pursuing political interests[44] and significantly affects the restriction of freedom of expression online – for example, through the adoption of restrictive legislation or the implementation of tools that, under the guise of combating disinformation, are in fact used to surveil citizens[45]. While the blocking and removal of content promoting terrorism and extremism can – and indeed should – be considered legitimate, more controversial are cases such as that of Pakistan, where content deemed blasphemous or critical of the judiciary has been removed; Turkey, where statements

41 B. Trish *„Big Data under Obama and Trump: The Data-Fueled U.S. Presidency". Politics and Governance* (ISSN: 2183-2463), ed. Cogitatio Press, Lisbon 2018, vol. 6, s. 29-38.

42 K. Izdebski, *Walka z dezinformacją oraz przejrzystość reklam politycznych w przestrzeni internetowej*, [in:] M. Bernaczyk, T. Gąsior, J. Misiuna, M. Serowaniec (eds.), *Znaczenie nowych technologii dla jakości systemu politycznego – ujęcie politologiczne, prawne i socjologiczne*, Wydawnictwo Naukowe Uniwersytetu Mikołaja Kopernika, Toruń 2020, p. 170.

43 Ibid., p. 172.

44 In an era of information overload and a lack of effective verification mechanisms, it is difficult to determine whether statements made by a politician -statements that may even align with Russian propaganda – are deliberate acts or simply the result of unawareness of the risk that such remarks could be used contrary to the author's intent. Source: M. Marek, *Operacja Ukraina – Kampanie dezinformacyjne, narracje, sposoby działania rosyjskich ośrodków propagandowych przeciwko państwu ukraińskiemu w okresie 2013–2019*, Wydawnictwo Difin SA, Warszawa 2020, p. 128.

45 M. Danek, *Modele walki z dezinformacją…*, op. cit., p. 135.

defamatory of Mustafa Kemal Atatürk have been censored; or Russia, where content related to unauthorised protests or challenging the territorial integrity of the Russian Federation has been taken down. This should not, however, discourage efforts to combat the spread of false information in cyberspace, nor should it undermine recognition of the impact disinformation has on political and social systems[46]. One of the most prominent examples of disinformation spread within the Polish internet space is the case of the computer game Blue Whale, which was alleged to encourage children on a mass scale to commit suicide. The story, originally published by the newspaper The Sun and subsequently reported by Polish media (and, unsurprisingly, widely shared on social media), prompted a response from the Ministry of National Education, which issued a warning to schools. This situation highlighted how media exaggeration can influence the political decision-making process. The above example demonstrates that online disinformation poses a potential threat both to social security and to the functioning of the political system. However, the fundamental issue remains how to combat this phenomenon effectively without infringing upon freedom of expression[47]. The current pace of technological development–often described as the fastest in human history and referred to as a revolution–has resulted in a situation where political spheres and state institutions do not always keep up with the rate of change. As a consequence, the actions they undertake do not shape the emerging reality, but rather constitute a post-factum response[48].

In this context, it is worth noting the legal measures undertaken by Germany and France to combat fake news in cyberspace. On 1 January 2018, the restrictive provisions of Germany's Network Enforcement Act (NetzDG) came into force. The act imposes an obligation on social media platforms with more than two million users to promptly remove posts reported by users as inciting hatred. These platforms are required to delete such posts within 24 hours, although the deadline may be extended to seven days if the content is subject to dispute. Failure to comply may result in financial penalties of up to €50 million. The law was widely criticised by the then parliamentary opposition as well as by representatives of Facebook in Germany. In France, meanwhile, in accordance with earlier announcements by President Emmanuel Macron, the National Assembly passed a law in November 2018 that, during the pre-election period and throughout elections, obliges online platforms to publicly disclose the identity of entities purchasing sponsored political content, along with the amount of money spent for this purpose. As it soon turned out, the French government itself became a victim of this legislative solution when Twitter France announced it would not unilaterally determine which content qualified as political, and consequently blocked all such advertising in France – including a government-sponsored voter turnout campaign ahead of the European Parliament elections[49]. In Singapore, the authori-

46 Ibid., p. 136.

47 M. Danek, *Modele walki z dezinformacją…*, op. cit., p. 137.

48 Ibid., p. 138.

49 Ibid., pp. 139–140.

ties have implemented legislation containing a very broad definition of what may be arbitrarily classified as fake news. This includes, for example, statements that influence the outcome of presidential or parliamentary elections or referendums, as well as content that undermines public confidence in the performance of any duty, function, or power by the government or any other state authority. The dissemination of such content is punishable by a fine of up to 1 million Singapore dollars (approximately 735,000 USD) or up to ten years of imprisonment[50].

The above examples clearly demonstrate that combating disinformation in cyberspace is not an easy task and cannot be achieved through a single political decision or isolated political action. Countering cyber threats requires the creation of a system composed of effective processes aimed at mitigating such risks, which, in turn, necessitates cooperation between state institutions, private entities, and society as a whole.

Conclusions

Contemporary threats to national security also reside in cyberspace. Disinformation is a key tool used to weaken the defence capabilities of states. Since 2014, there has been a marked increase in offensive cyber activity carried out by entities operating within Russian state structures, or on their behalf, conducting large-scale disinformation campaigns primarily targeting NATO and EU member states. Among the most significant consequences of Russia's hybrid operations in cyberspace are the discrediting of EU and NATO member states, the fuelling of historical antagonisms, the pursuit of societal division, the obstruction of cooperation and decision-making processes, and the consolidation of pro-Russian circles within target countries.

The search for appropriate methods and effective means of ensuring both individual and collective security in the Republic of Poland has become a priority not only for national governments but also for international organisations[51].

In conclusion, it must be acknowledged that in order to enhance the level of state security, it is essential to develop a disinformation counteraction system that relies on close cooperation between state institutions, private actors, and society at large. Fact-checking initiatives have demonstrated that rapid responses to false content – as well as its removal from media and digital spaces – contribute to improving the overall security of the information creation and distribution system[52]. At the individual level, actions should be taken to enable the partial distinction between true and false content. The method for verifying the credibility of information is based on four fundamental elements: assessment of the source, the fact, the image, and the timeliness.

Disinformation on the internet poses a potential threat both to social security and to the functioning of the political system. a solution should be developed to ensure

50 M. Danek, *Modele walki z dezinformacją…*, op. cit., p. 134.

51 T. Goryca, *Theory and Practical Aspects of State Authorities Protection Organization*, *Security Forum* 2021, no. 2, Wydawnictwo Akademia WSB, Dąbrowa Górnicza 2021, p. 55.

52 Ibid., p. 14.

oversight of the targeting and microtargeting of political advertisements. To this end, the Code of Practice of the European Commission may serve as a reference, as it obliges online platform operators to make information on targeting and microtargeting publicly accessible, and to provide users with clear explanations as to why a given advertisement – including political advertising – is directed specifically at them.

In combating disinformation and in the field of media education, the state plays a key role. Actions in this area must encompass all levels of education – primary, secondary, and higher. a particularly important role is also played by media representatives, as well as members of the academic and expert communities, who bear the responsibility of supporting the state in countering disinformation. Cooperation should be established between state institutions and other entities responsible for education in order to build the necessary infrastructure to address this phenomenon. It is essential to introduce institutional and legislative systemic solutions that will, to some extent, immunise the state – and thus its citizens – against the growing spread of disinformation in the media.

Bibliography

Bączek P., *Dezinformacja jako zagrożenie dla bezpieczeństwa informacyjnego współczesnych społeczeństw*, *Security Review*, Wydawnictwo Instytut Analizy Ryzyka Sp. z o. o., Rzeszów 2020, no. 4 (17).

Bączek P., *Wyzwania i zagrożenia dezinformacyjne w kontekście rozwoju sztucznej inteligencji*, [in:] W. Fehler (ed.), *Informacyjny Wymiar Bezpieczeństwa Państw i Jednostek*, Wydawnictwo Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach, Siedlce 2021.

Bennet W. L., Livingston S. (eds.), *The Disinformation Age: Politics, Technology and Disruptive Communication in the United States,* Cambridge University Press, Cambridge 2021.

Chałubińska-Jentkiewicz K., *Droga do regulacji? Dezinformacja w przekazie medialnym*, [in:] K. Chałubińska-Jentkiewicz, M. Nowikowska, K. Wąsowski (eds.), *Media w erze cyfrowej. Wyzwania i zagrożenia*, Wydawnictwo Wolters Kluwer, Warszawa 2021.

Cyuńczyk F., Walka z dezinformacją w warunkach kryzysu praworządności, [in:] K. Stasiuk-Krajewska, M. Wenzel (eds.), Dezinformacja w czasach kryzysu, Wydawnictwo Adam Marszałek, Toruń 2024.

Czupryński A., Wiśniewski B., Zboina J. (eds.), *Bezpieczeństwo. Teoria–Badania–Praktyka,* Centrum Naukowo-Badawcze Ochrony Przeciwpożarowej im. Józefa Tuliszkowskiego – Państwowy Instytut Badawczy, Józefów 2015.

Czupryński A., Wiśniewski B., Zboina J. (eds.), *Nauki o bezpieczeństwie. Wybrane problemy badań,* Centrum Naukowo-Badawcze Ochrony Przeciwpożarowej im. Józefa Tuliszkowskiego – Państwowy Instytut Badawczy, Józefów 2017.

Danek M., *Modele walki z dezinformacją: od restrykcji do współpracy*, [in:] M. Bernaczyk, T. Gąsior, J. Misiuna, M. Serowaniec (eds.), *Znaczenie nowych technologii dla jakości systemu politycznego – ujęcie politologiczne, prawne i socjologiczne*, Wydawnictwo Naukowe Uniwersytetu Mikołaja Kopernika, Toruń 2020.

DiResta R., Grossman S., *Potemkin Pages & Personas: Assessing GRU Online Operations, 2014–2019*, ed. Stanford Cyber Policy Center, Stanford 2019.

Gliwa S., *Terroryści w sieci – media społecznościowe w służbie propagandy ISIS*, Wydawnictwo Towarzystwa Wiedzy Obronnej, Warszawa 2021.

Golka M., *Bariery w komunikowaniu i społeczeństwo (dez)informacyjne*, Wydawnictwo Naukowe PWN, Warszawa 2008.

Goryca T., *Risk and Threats in Protective Measures of the Units Responsible for Security of Executive State Bodies*, *Security Forum* 2022, no. 1, Wydawnictwo Akademia WSB, Dąbrowa Górnicza 2022.

Goryca T., *Selected Operational and Intelligence Activities as Elements of State Bodies*, *Security Forum* 2024, no. 1, Wydawnictwo Akademia WSB, Dąbrowa Górnicza 2024.

Goryca T., *Theory and Practical Aspects of State Authorities Protection Organization*, *Security Forum* 2021, no. 2, Wydawnictwo Akademia WSB, Dąbrowa Górnicza 2021.

Izdebski K., *Walka z dezinformacją oraz przejrzystość reklam politycznych w przestrzeni internetowej*, [in:] M. Bernaczyk, T. Gąsior, J. Misiuna, M. Serowaniec (eds.), *Znaczenie nowych technologii dla jakości systemu politycznego – ujęcie politologiczne, prawne i socjologiczne*, Wydawnictwo Naukowe Uniwersytetu Mikołaja Kopernika, Toruń 2020.

Janik K., *Państwo, Polityka, Bezpieczeństwo Wewnętrzne*, Wydawnictwo Adam Marszałek, Toruń 2021.

Kaczmarczyk B., Wiśniewski B., Gwardyński R., *Security of an Individual*, *Zeszyty Naukowe Państwowej Wyższej Szkoły Zawodowej im. Witelona w Legnicy*, no. 3 (28) 2018, Legnica 2018.

Khan A., Brohman K., Addas S., *The Anatomy of "Fake News": Studying False Messages as Digital Objects*, *Journal of Information Technology*, Sage, 2022, vol. 37, iss. 2.

Kowalska-Chrzanowska M., Krysiński P., Pamuła N., *Metody i narzędzia budowania społecznej odporności na dezinformację: od fact-checkingu po edukację medialną*, Wydawnictwo Naukowe Uniwersytetu Mikołaja Kopernika, Toruń 2024.

Kupiecki R., Bryjka F., Chłoń T., *Dezinformacja międzynarodowa – Pojęcie, Rozpoznanie, Przeciwdziałanie*, Wydawnictwo Naukowe Scholar, Warszawa 2022.

Kuś J., *Zjawisko dezinformacji z perspektywy psychologicznej: uwarunkowania i przeciwdziałanie*, [in:] K. Stasiuk-Krajewska, M. Wenzel (eds.), *Dezinformacja w czasach kryzysu*, Wydawnictwo Adam Marszałek, Toruń 2024.

Marek M., *Operacja Ukraina – Kampanie dezinformacyjne, narracje, sposoby działania rosyjskich ośrodków propagandowych przeciwko państwu ukraińskiemu w okresie 2013–2019*, Wydawnictwo Difin SA, Warszawa 2020.

Miodek M. *(ed.), Dialog w Unii Europejskiej – scenariusze zajęć dydaktycznych z zakresu komunikacji, mediacji, stereotypów i przeciwdziałania dezinformacji,* Wydawnictwo Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław 2022.

Nowak T., *Działania hybrydowe w cyberprzestrzeni prowadzone przez Rosję jako zagrożenie dla bezpieczeństwa euroatlantyckiego*, [in:] M. Banasik, A. Rogozińska (eds.), *Zagrożenia Federacji Rosyjskiej i Bezpieczeństwo Międzynarodowe*, Wydawnictwo Difin SA, Warszawa 2020.

Nowak T., *Polityka Unii Europejskiej w latach 2014–2019 wobec działań hybrydowych Federacji Rosyjskiej*, [in:] M. Banasik, A. Rogozińska (eds.), *Zagrożenia Federacji Rosyjskiej i Bezpieczeństwo Międzynarodowe*, Wydawnictwo Difin SA, Warszawa 2020.

Proposal for a Regulation of the European Parliament and of the Council on ENISA, repealing Regulation (EU) No 526/2013, and on cybersecurity certification of information and communication technologies (OJ EU C 227/13 of 28.6.2018).

Rejman B., Rejman K., *Fake news jako narzędzie działań dezinformacyjnych a bezpieczeństwo współczesnych systemów społeczno–ekonomicznych*, [in:] K. Rejman, M. Wilczyńska, J. Wołejszo (eds.), *Bezpieczeństwo Informacji Wobec Współczesnych Zagrożeń*, Wydawnictwo Kaliskie Towarzystwo Przyjaciół Nauk, Kalisz 2023.

Stasiuk-Krajewska K., *Dezinformacja. Próba ujęcia dyskursywnego*, *Media – Kultura – Biznes*, Wydawnictwo Uniwersytet Gdański, Gdańsk 2023, vol. 1 (14).

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2020.

Szulc M., *Manipulowanie informacją w sieci za pomocą fake newsów jako zagrożenie dla młodzieży*, [in:] *Psychologia Wychowawcza*, Wydawnictwo Uniwersytet Gdański, Gdańsk 2020, vol. 599730, no. 17.

Tomaszewski S., *Media elektroniczne jako instrument walki informacyjnej*, [in:] W. Fehler (ed.), *Informacyjny Wymiar Bezpieczeństwa Państw i Jednostek*, Wydawnictwo Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach, Siedlce 2021.

Trish B., *Big Data under Obama and Trump: The Data-Fueled U.S. Presidency, Politics and Governance* (ISSN: 2183-2463), Cogitatio Press, Lisbon 2018.

Wisniewski B., Prońko J., *Ogniwa ochrony państwa*, Akademia Obrony Narodowej, Warszawa 2003.

Wiśniewski B., Sander G. S., *Zagrożenie, kryzys i sytuacji kryzysowa – jako uwarunkowania życia współczesnego człowieka*, "Bezpieczeństwo i Technika Pożarnicza", Nr 1/2016, Centrum Naukowo-Badawcze Ochrony Przeciwpożarowej Państwowy Instytut Badawczy, Józefów 2016.

Wojnowski M., *Mit „wojny hybrydowej". Konflikt na terenie państwa ukraińskiego w świetle rosyjskiej myśli wojskowej XIX–XXI wieku*, [in:] *Przegląd Bezpieczeństwa Wewnętrznego. Wojna hybrydowa – Wydanie Specjalne*, Wydawnictwo Agencji Bezpieczeństwa Wewnętrznego, Wiązowna 2015.

Wyzwania, szanse, zagrożenia i ryzyko dla bezpieczeństwa narodowego RP o charakterze wewnętrznym, R. Jakubczak, B Wiśniewski (red. nauk.), Wyższa Szkoła Policji w Szczytnie, Szczytno 2016.

About the Author

Marek Przybyła – his academic work focuses on issues of public security, the improvement of information security systems, and matters related to cybersecurity in the context of individuals and facilities of critical importance to the functioning of the state.