sciendo

STUDIES IN LOGIC, GRAMMAR AND RHETORIC 70 (83) 2025

DOI: 10.2478/slgr-2025-0059

Anna Grabowska-Siwiec
University of Białystok
Poland
e-mail: a.grabowska-siwiec@uwb.edu.pl
ORCID: 0000-0003-0788-4171

RUSSIAN AND BELARUSIAN DISINFORMATION OPERATIONS TARGETING POLAND AND SELECTED NATO MEMBER STATES[1]

Abstract. The subject of the article is the common experience of disinformation in Poland and selected NATO countries. Disinformation is defined in the context of state security and as a tool used by state agencies to achieve the goals set out by political authorities. The analysis included publicly available reports of the agencies responsible for state security, both Polish and those of other members of the North Atlantic Treaty Organisation (NATO). The research question posed in the article is: are the same methods of disinformation used against Poland and other NATO member states and what issues do they concern? The article primarily uses the method of analysis and comparative analysis of the above-mentioned reports and information materials from security agencies, both intelligence and counterintelligence. The mechanisms of counteracting and combating disinformation are exposed and recommendations for combating disinformation are made.

Keywords: disinformation, NATO, intelligence, information warfare.

Introduction

Because of the various ongoing conflicts around the world, online disinformation has become a dominant tool for manipulating societies. Cyberspace makes it not only a low-cost instrument, but also one that spreads extremely rapidly. Changes in habits and the shifting of many aspects of life online, especially among young people, ensure the effectiveness of online disinformation by enabling it to spread through sharing, reposting, and 'liking.' The mechanisms of disinformation are universal, which further contributes to its efficacy. Its role in advertising, business, or market competition is just one of its facets. Another is the use of disinformation to disrupt a nation's sense of security, destabilise states, and sow chaos. In this re-

gard, disinformation is an important tool for broadly understood security structures, including state intelligence agencies and bodies established to support military operations. In the field of security, disinformation serves as a means to carry out specific actions and achieve concrete objectives.

In this article, disinformation will be discussed specifically in the context of state security and as a tool used by state agencies to achieve objectives set out by political authorities. The analysis will cover publicly available reports from agencies responsible for state security, both Polish and those of other members of the North Atlantic Treaty Organisation (NATO): the 2023 Report of the Estonian Foreign Intelligence Service; the 2022–2023 Report of the Estonian Internal Security Service (Kaitsepolitseiamet, KAPO[2]); the 2023 report of the Canadian Security Intelligence Service (CSIS); information from the Czech special service – the Security Information Service (BIS); information from the United States Federal Bureau of Investigation (FBI); information from the Plenipotentiary of the Government for the Security of the Information Space of the Republic of Poland, Stanisław Żaryn, as published on the gov.pl website; data from Poland's Internal Security Agency (ABW); the 2023 Report of the Government Plenipotentiary for Cybersecurity; as well as materials published on the websites of the North Atlantic Treaty Organisation (NATO).

The research question posed in the article is: are the same methods of disinformation used against Poland and other NATO member states, and what topics do they concern? The article primarily utilises the method of analysis and comparative analysis of the aforementioned reports and informational materials released by security agencies, both intelligence and counterintelligence. This analysis was conducted with the aim of identifying the methods and means employed by state intelligence agencies to carry out disinformation activities and actively counteract them. In addition, reliable inference was used, assuming that the reports and information from security agencies utilised in the research contain accurate data that leads to correct conclusions.

The Concept of Disinformation

The concept of 'disinformation' is present in the security sphere across various domains. The "NATO Glossary of Terms and Definitions" (Słownik terminów i definicji NATO, 2024) provides an extensive definition, describing disinformation as "Any undertaking intended to mislead the adversary by manipulating, feigning actions, and fabricating evidence, in or-

der to provoke actions detrimental to their own interests." At the same time, it also points to electronic disinformation as a category of electronic countermeasure aimed at disrupting, dispersing, and misleading the adversary or their electronic systems (Słownik terminów i definicji NATO, 2024). Katarzyna Bąkowicz (Bąkowicz, 2023, p. 11) maintains that disinformation is neither truth nor lie; its essence lies in the fact that the content contains true elements, although it is not true itself. She also emphasises that disinformation is a process that unfolds over time and appeals to our emotions, worldview, authorities, as well as the dynamically changing reality.

Disinformation is often associated with the concept of information manipulation and information warfare. A scholar of this subject, Tomasz R. Aleksandrowicz (Aleksandrowicz, 2021, p. 50) states that disinformation involves conveying (most often true) information in such a context that the recipient draws conclusions aligned with the intentions of the attacker. By defining disinformation in this way, he points to its use as an offensive tool. Certain specific features of disinformation can be pointed out in the context of activities that have the characteristics of conflict or offensive actions. Disinforming entails transmitting information, be it true or false, in a way that misleads an opponent or competitor and prompts them to act in accordance with our expectations and to our advantage. Thus, disinformation is not simply a lie or the transmission of false information. T.R. Aleksandrowicz states that disinformation is a form of deception (Aleksandrowicz, 2021, p. 52). Actions involving disinformation rarely concern a single piece of information; typically, it is a disinformation campaign utilising a whole conglomerate of information, the majority of which is true, with perhaps one crucial (for achieving the intended effect) bit of it being false. Sometimes a disinformation campaign is conducted on the basis of true information but presented in a way that makes them seem false. The effectiveness of disinformation increases when several independent sources and information channels are used (Aleksandrowicz, 2021, p. 50).

It is possible to achieve a variety of objectives through disinformation, including influencing the opponent's state institutions and society; impacting actions, events, and conditions within the adversary's country; as well as discrediting it. The targets of such activities may also vary and may include: the government, the general public, or particular social groups. The ultimate effect of disinformation is to shape perception, resulting in the victim of disinformation taking actions that benefit the perpetrator (Minkina & Gałek, 2015, pp. 36–37, 39).

Although disinformation as an operational tactic has been known for centuries, the arena in which it is practised has changed in modern times.

Its effective and widespread use has become possible with the emergence of technical capabilities for shaping the information sphere on a global scale, practically by any entity with access to the internet, understood as a communication platform. The internet has enabled anyone to potentially reach an unlimited number of recipients and provides the technical means to falsify information, for example through identity theft or the creation of fake messages masquerading as genuine ones (e.g. deep fakes) (Aleksandrowicz, 2021, pp. 54–55). Fake news is not a lie. It is manipulated information, albeit not necessarily false, having undergone specific processing. Structurally, it is identical to genuine news (Bąkowicz, 2023, pp. 48–49).

Disinformation employs a range of mechanisms, including the information bubble, the echo chamber, and the spiral of silence. These are described by Katarzyna Bąkowicz, mentioned above. When searching for information, we face the challenge of prioritising by importance. Algorithms are supposed to assist us in this regard. In theory, they organise the world of knowledge according to what we need. The algorithm first defines our preferences (based on our queries) and then, using this basis, filters the content made available to us. What initially seems pleasant, like receiving only information consistent with our beliefs, over the longer term poses a serious threat to our security. This is because we surround ourselves with only one type of content, losing sight of the full spectrum of information (Bąkowicz, 2023, pp. 26–27). Gradually, we become cut off from other news, thus closing ourselves off to new ideas or solutions, often without even realising we are taking part in this process (Bąkowicz, 2023, p. 71). As a result we close ourselves off in an information bubble.

Remaining within an information bubble also exposes us to the echo chamber effect. This occurs when our environment continually generates new content that aligns with our own views. Disinformation is a fundamental component of the echo chamber and contributes to distorting our perception of the world, making it impossible to truly understand it (Bąkowicz, 2023, pp. 74–75).

Remaining in an information bubble also puts us in danger of repeating and popularising views that are in agreement with those of the group we are in contact with. We are more willing to express opinions that will be approved by the group, while we are reluctant to voice those that might be disapproved of by the rest of the group. This phenomenon is called the spiral of silence. It was described by Elisabeth Noelle-Neumann, who stated that people are more inclined to follow opinions that appear to be dominant, even if they are not grounded in reality (Noelle-Neumann, 2004, pp. 22–23).

This behaviour carries with it a risk of disinformation, as this rule does not depend on whether the group adheres to the truth.

These mechanisms are common tools of propagating disinformation used by state actors, including intelligence services, to pursue their objectives.

The Use of Disinformation against Poland

In a 2023 report the Government Plenipotentiary for Cyber Security pointed out that in that year Poland was the target of numerous cyberattacks, including operations conducted by hostile state agencies, aimed at obtaining key information, probing ICT system for the purpose of potential future damaging cyberattacks, disrupting critical infrastructure and key resources, as well as spreading disinformation with the purpose of propagating false information and foreign narrations, and sowing social division (Sprawozdanie Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa za 2023 rok, 2023, p. 8). Examples of disinformation used against Poland and other NATO countries can be traced based on, among others, reports of member states' security agencies.

It should be noted here that in this context the study invokes the Polish term *służby specjalne* (which can be translated as 'special services,' 'security services,' 'security agencies,' 'security apparatus,' 'intelligence services' depending on context – translator's note), which is strictly defined in Polish law, in the act on ABW and AW (Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, Dz. U. 2025, poz. 902). The act lists these "special services," which include: *Agencja Bezpieczeństwa Wewnętrznego* (ABW – Internal Security Agency), *Agencja Wywiadu* (AW – Foreign Intelligence Agency), *Służba Kontrwywiadu Wojskowego* (Military Counterintelligence Service), Służba Wywiadu Wojskowego (Military Intelligence Service), and Centralne Biuro Antykorupcyjne (Central Anti-Corruption Bureau). Whereas in academic circles a number of definitions have been developed, which boil down to services responsible for performing intelligence and counterintelligence tasks (Zalewski, 2005) (Hoc, 2002, p. 42).

The special services main tools are operational and reconnaissance measures. According to Tomasz R. Aleksandrowicz, an additional feature should be included in this definition to clearly distinguish this type of state service. He points to their authority to undertake actions not only in cases where a crime is suspected, but also in any situation that is associated with a threat to state security. (Aleksandrowicz, 2013, p. 255).

While internal services – counterintelligence – in a democratic system may operate in situations of "reasonable suspicion of a crime," in non-democratic systems this is not so clear-cut. This is particularly the case when it comes to intelligence services – that is, the security agencies which operate in the external sphere of the state. Their primary task is to collect information, which, once analysed, is then passed on to decision-makers. They may also carry out active operations. These include, among others: creating situations favourable to the state, misleading the opponent (disinformation), recruiting agents of influence, compromising the opponent, and assassinations. (Aleksandrowicz, 2013, p. 257).

As indicated above, NATO views disinformation as the deliberate creation and dissemination of false or manipulated information with the intention of deceiving or misleading. The term "disinformation" is commonly used as a general expression referring to a wide range of tactics, techniques, and procedures, which the alliance defines as "hostile information activities". These are intended to deepen divisions within and between NATO member states and ultimately weaken the Alliance. (NATO's approach to counter information, 2025). This is the primary objective of Russia's disinformation activities. This is acknowledged by many member states, including Poland.

The disinformation campaigns targeting Poland were reported on by the spokesperson for the Minister-Coordinator of Special Services and by the Government Plenipotentiary for the Security of the Information Space of the Republic of Poland, Stanisław Żaryn, on the gov.pl website, where one can find 31 Situation Reports concerning "disinformation against Poland," relating to events in 2023 (9 February – 3 December). (Dezinformacja przeciwko Polsce, 2023). Among the numerous examples of information attacks, mainly by the Russian Federation and Belarus, the reports also list specific examples of disinformation attacks against Poland:

- Portraying Poland as a country seeking to seize Western Ukraine, the Grodno region, and even to launch a kinetic attack on the Kaliningrad Oblast (Meldunek sytuacyjny 07/04/2023, 2023). In this context, disinformation messages claimed that Poland's support for Ukraine is "disingenuous," calculated to ultimately weaken it and occupy its western territories (Meldunek sytuacyjny 21/04/2023, 2023),
- Portraying Poland as a militarily weak state, exhausted from aiding Ukraine (Meldunek sytuacyjny 09/02/2023, 2023),
- Portraying Poland as a troublemaker in Europe, destabilising the Old World's security (Meldunek sytuacyjny 21/04/2023, 2023) (Meldunek sytuacyjny 23/02/2023, 2023),

- Accusing Poland of murdering migrants on the Polish-Belarusan border (Meldunek sytuacyjny 17/03/2023, 2023),
- Portraying Poland as forcing western states to become more deeply involved in military aid for Ukraine (Meldunek sytuacyjny 21/04/2023, 2023),
- Suggesting that Polish authorities are sending mercenaries to Ukraine to sustain the armed conflict (Meldunek sytuacyjny 28/04/2023, 2023) (Meldunek sytuacyjny 27/08/2023, 2023),
- Accusing Poland of blowing up Nord Stream1 and Nord Stream2 (Meldunek sytuacyjny 20/05/2023, 2023),
- Based on a video of an explosion in the vicinity of Khmelnytskyi (Ukraine), the Kremlin distributed information about a radioactive cloud allegedly moving over Poland, while simultaneously claiming that the cloud was formed after the destruction of uranium ammunition given to the Armed Forces of Ukraine by the West (Meldunek sytuacyjny 26/05/2023, 2023),
- Discrediting refugees from Ukraine, attributing negative characteristics to them (Meldunek sytuacyjny 03/06/2023, 2023),
- Poland as a provocateur destabilizing Europe on behalf of the United States (Meldunek sytuacyjny 17/06/2023, 2023),
- "*resurgent fascism*" in Poland and the Baltic states, a thesis accompanied by accusations of human rights violations and racism, as demonstrated by the different treatment of refugees from Ukraine and the people trying to cross from Belarus due to their place of origin (Meldunek sytuacyjny 27/08/2023, 2023),
- discrediting NATO troops stationed in Poland by pointing out that they pose a threat to its independence and security (Meldunek sytuacyjny 02/09/2023, 2023).

This list does not exhaust the range of topics raised by Russia and Belarus regarding Poland. This is a subjective selection of issues compiled on the basis of data provided by the special services to the Government Plenipotentiary for Information Space Security of the Republic of Poland, Stanisław Żaryn. It is worth emphasising that some disinformation content is repeated regularly, whilst other pieces of it appear once or over a short time period. Those that are continuously "fed" into the infosphere decidedly include emphasising Poland's military weakness, its harmful actions towards Ukraine, aimed not at supporting Ukraine but at securing its own particular benefits, and unethical conduct towards migrants on the border with Belarus.

One can find examples of disinformation operations directed against Poland among the announcements published on the ABW's website. In May 2021, its officers detained two people in the Łódź Voivodeship sus-

pected of disrupting the ICT network. The detainees organized an ICT infrastructure, consisting of modems and devices cooperating with a large number of SIM cards, which ensured the anonymization of phone calls and activities performed on the Internet, as well as obscuring the data of the people using the network. The Internal Security Agency stated that this infrastructure was used, among others, by foreign special services, for disinformation activities carried out in Poland (Umożliwiali prowadzenie dezinformacji. Zatrzymała ich ABW, 2021) (there is no data on the content of the disinformation). In October 2023, the National Prosecutor's Office initiated an investigation, based on the Internal Security Agency's own materials on the suspicion of disinformation being spread on behalf of foreign intelligence, consisting of disseminating false or misleading information aimed at causing serious disruptions to the constitutional order of the Republic of Poland, i.e. an offence under Article 130 § 9 of the Criminal Code. These activities involved impersonating the Law and Justice political party during the election campaign. The hostile activities in cyberspace identified by the Internal Security Agency bear, in the assessment of this service, the hallmarks of an attempt to influence the course of elections in Poland. (Komunikat ABW z dn. 12 października 2023 r., 2023).

Poland also cooperates with partner countries from the EU and NATO in combating disinformation activities on an international scale. One example of such operations were procedural measures, including searches carried out in Warsaw and Tychy on 27 March 2024, as part of an investigation into uncovered espionage activities conducted on behalf of the Russian Federation, directed against the states and institutions of the European Union. This was the result of international cooperation between the Internal Security Agency (ABW) and a number of European services, coordinated in particular with partners from the Czech Republic. As a result, activities aimed at organising pro-Russian initiatives and media campaigns in EU member states were documented. Their objective was to implement the assumptions of the Kremlin's foreign policy, including the weakening of Poland's position on the international stage, discrediting Ukraine, and tarnishing the image of European Union institutions. (Informacja, 28.03.2024, 2024).

Disinformation against other NATO member states

The available reports of the special services of some NATO members clearly indicate specific disinformation activities undertaken against them by Russia. In its 2023 report, the Estonian Foreign Intelligence Service

points out, among others, disinformation activities such as glorifying Russia and discrediting Estonia and other Western countries (International Security and Estonia, 2023, p. 48). In 2023, the Estonian Internal Security Service KAPO (Kaitsepolitseiamet) recorded disinformation activities targeting the presence of NATO forces and the enlargement of the Alliance. Rumours were spread across Estonian social media platforms alleging that allied soldiers were raping girls in Võrumaa, and claims were made that the police had taken no action to address these incidents. (Annual Review 2022–2023 Estonian Internal Security Service, 2023, p. 7).

Disinformation is also an element of hybrid warfare. In the cited report, KAPO points out that Russia fuels social tensions in neighbouring countries through hybrid activities, and it can be expected that it will use any and all means that would not trigger NATO's collective defence clause yet still allow it to pursue its intended objectives. Such measures included an operation carried out in autumn 2023 in hundreds of schools in Estonia and other Baltic states. They received emails claiming that explosive devices had been placed in school buildings. Similar bomb threats were also sent to several other institutions in Estonia. The aim was not only to disrupt their functioning but also to create a sense of danger and psychological and emotional tension by targeting children, undermining trust in the state and its security structures. (Annual Review 2022–2023 Estonian Internal Security Service, 2023, p. 13).

NATO member states' security agencies, including the cited Estonian reports, also note a strong disinformation campaign directed against Ukraine. They point out that since the very beginning of the conflict with Russia in 2014, Ukraine has been a constant target of disinformation spread by Russian special services. One of the objectives of this activity is to prevent the Ukrainian government from reliably informing the citizens of Ukraine about the situation in the country. Disinformation is intended to sow fear and mistrust towards the state's leadership, weaken societal resistance, and create informational noise that makes it difficult to distinguish reality from disinformation. Many of the messages directed at Ukrainian society are aimed at breaking the resistance of the Ukrainian population and creating the impression of Russia's overwhelming superiority. (International Security and Estonia, 2023, p. 13). In the cited report, the Estonians stated that the tools Russia uses to spread disinformation include cyberattacks (International Security and Estonia, 2023, p. 16).

The Canadian Security Intelligence Service (CSIS) also recorded disinformation activities conducted by Russian services in its territory in 2023. CSIS assesses that Canada's involvement in the conflict in Ukraine has led

to an intensification of disinformation efforts by the Russian Federation targeting Canadian society. These concern, among other things, the Russian narrative on the war in Ukraine, which seeks to discredit the West and promote Russian propaganda calling for the lifting of sanctions imposed by the West. In previous years as well, Canadian services had noted Russian activities aimed at discrediting the Ukrainian community in Canada, claiming that it included neo-fascists whose goal was to control Canada's foreign policy. According to CSIS analysts, disinformation carried out by Russian services in Canada supports the efforts of the Russian government to delegitimise and silence the diaspora originating from Eastern Europe, as well as to reinforce various hybrid operations conducted by Russia (CSIS Public Report 2023, 2023, p. 30).

The Canadians also noted that disinformation related to the conflict in Ukraine is spread by the Russian Embassy in Canada, through its social media.

The FBI, together with the Department of Justice, published a press release on its website relating to combating disinformation. On 9 July 2024, the FBI, along with other services, including Canadian ones, seized the names of two domains and searched 968 social media accounts used by Russian actors to create a bot farm on social media. The bot farm, powered by artificial intelligence, was spreading disinformation in the United States and abroad. This was an unprecedented action by the American agencies aimed at halting the dissemination of disinformation intended to sow discord in the United States and allied countries. Among others, the Americans identified messages relating to the following topics:

- President Vladimir Putin's statements justifying Russia's actions in Ukraine,
- V. Putin's statements indicating that certain geographical areas of Poland, Ukraine, and Lithuania were "gifts" to these countries from the Russian forces that liberated them from Nazi control during World War II,
- Data indicating that the number of foreign soldiers serving in Ukrainian forces is much lower than public estimates,
- Vladimir Putin's statements that the war in Ukraine is not a territorial conflict or a matter of geopolitical balance, but rather one of "the principles on which the New World Order will be based".

This content was published by the bot farm between October and November 2023 and considered by the US authorities to be a disinformation narrative pushed by the Russian government (Justice Department Leads Efforts Among Federal, International, and Private Sector Partners to Disrupt Covert Russian Government-Operated Social Media Bot Farm, 2024).

Czech authorities describe Russian disinformation operations, along with hybrid intelligence operations, in the context of war in strategic documents on state security, including the 2015 Security Strategy (Czarnecki, 2023, p. 35). Whereas the Information Security Service of the Czech Republic (BIS) describes disinformation as one of the biggest threats to democracy in the Czech Republic (Czarnecki, 2023, p. 40). The BIS recorded an increase in Russian disinformation in the Czech Republic in the period of 2014–2016. It pointed out that the actions of (pro)Russian activists involved in spreading false information posed one of the most serious threats to the state after 2014. (Bezpečnostní informační služba, Zpráva o činnosti za 2018, 2018) Along with disinformation operations, cyberattacks were carried out against the Ministry of Foreign Affairs and the Army of the Czech Republic (Bezpečnostní informační služba, Zpráva o činnosti za 2018, 2018).

Szczepan Czarnecki, an analyst at the Institute of Eastern Europe, divides the disinformation aimed against the Czech Republic after the outbreak of the war in Ukraine into two content groups. The first is fake news about the war in Ukraine and the Ukrainian authorities, the second is so-called migration disinformation (Czarnecki, 2023, p. 23). The latter related directly to refugees from Ukraine. Numerous manipulated or decontextualised photos, videos, and texts appeared on various websites and discussion forums, attempting to portray refugees as criminals, radicals, or people with "low cultural capital" (troublemakers, vandals, etc.) The refugee issue was addressed alongside local economic and political problems, which diverted attention away from the Russian invasion itself. These activities led to a decline in the average citizen's interest in state policy, fostered distrust towards the authorities, and resulted in Ukrainians being blamed for Czech economic problems (Czarnecki, 2023, p. 23).

A lot of information has also appeared in the media space of the Czech Republic regarding the supply of weapons from the Czech Republic to Ukraine, which would prolong the war and prevent peace negotiations, and thus the end of the war (Czarnecki, 2023, p. 24). NATO also recognises the use of disinformation as a tool to promote false claims regarding the impact of warfare on climate change. According to alliance analysts, malign actors, including Russia, seek to weaken public pressure and political will to implement ambitious climate policies. They also undertake actions aimed at diverting attention and reducing resources allocated to climate adaptation and mitigation efforts. NATO analysts have concluded that these actors are supported by the Kremlin. Russian state media likewise routinely work to undermine confidence in climate change, portraying the phenomenon as

exaggerated or even beneficial. They present global warming as a "hoax" and emissions reduction plans as a form of "Western imperialism" designed to weaken the development of emerging economies. Russia denies the impact of pollution on climate change because of the strong links between its political powers and the state-controlled fossil fuel industry, which remains the primary source of state revenue. NATO has observed a significant increase in Russian disinformation related to Europe's green energy transition since the beginning of the full-scale Russian invasion of Ukraine. According to the alliance, between May 2022 and May 2024, Russia was the main driver of hostile communications about green energy across social media and online news outlets. (NATO Climate Change and Security Impact Assessment, 2024, p. 27).

Mechanisms to counter and combat disinformation

The aforementioned examples of disinformation, aside from originating primarily from Russia and echoing its narrative, in many cases also share similar contents. Recurring elements include blaming NATO for the conflict in Ukraine, questioning the alliance's intentions, "whitewashing" Russia, discrediting Ukrainian citizens, and portraying Poland as a "fascist" country allegedly planning to annex a part of Ukraine after the war.

The fact that different allied countries are both experiencing the problem of Russian disinformation and being targeted with similar narratives and mechanisms of their dissemination encourages undertaking joint allied actions in this area. Although not yet strictly defined in legal terms, joint initiatives to counter disinformation are already being implemented.

An example of such activity is the aforementioned operation involving the seizure of two domain names and the inspection of 968 social media accounts used by Russian actors to create bot farms. An integral part of this operation was the publication of a joint US–Canadian–Dutch cybersecurity advisory, prepared with the involvement of the FBI and the Cyber National Mission Force (CNMF), in cooperation with the Canadian Centre for Cyber Security (CCCS), the Netherlands General Intelligence and Security Service (AIVD), the Netherlands Military Intelligence and Security Service (MIVD), and the Dutch police. The advisory provides a detailed description of the technology behind the social media bot farm, including specifics of how its creators used a custom AI system to carry out the scheme. According to its authors, the advisory will enable social media platforms and researchers to identify and prevent further use of this technology by

the Russian government. In addition, X Corp. (formerly Twitter) voluntarily suspended the remaining bot accounts identified in court documents for violations of its terms of service. (Justice Department Leads Efforts Among Federal, International, and Private Sector Partners to Disrupt Covert Russian Government-Operated Social Media Bot Farm, 2024).

Another example of allied cooperation in combating disinformation is the aforementioned collaboration between the Internal Security Agency (ABW) and Czech security agencies. It led, among other things, to the identification of the international news portal *Voice of Europe*, which published articles, statements, commentaries, and interviews related to the current international situation, including Russia's war against Ukraine, with a biased, pro-Russian tone. The agencies established the method of financing of this operation and secured a number of electronic devices, including mobile phones (Informacja, 28.03.2024, 2024).

Cooperation between NATO member state's security agencies also has an educational dimension, whether through the joint publication of the aforementioned advisory or the release of press statements. Education is, after all, the fundamental method of building resilience against disinformation. KAPO highlights educational measures in its report. During the above-mentioned bomb threat crisis in Estonian schools, the Emergency Response Centre, the Rescue Board, and the Police and Border Guard Board explained the nature of the spam messages patiently and professionally to concerned individuals. Furthermore, as a result of these incidents, Estonian authorities decided to publicise the explanations from the Police and Border Guard Board and the Rescue Board on social media. This served to counter the spread of false information and prevent the spread of panic and of further disinformation. The cited KAPO report also provides contact details for institutions that should be reached in cases where there is suspicion that some content may be disinformation. (Annual Review 2022–2023 Estonian Internal Security Service, 2023, p. 13). The report is public and available online.

Since the dominant arena for disinformation activities is the internet and social media (Facebook, TikTok, Instagram, Telegram, X [Twitter], and others), many counter-disinformation measures are likewise centred on cyberspace. In the Czech Republic, state institutions block websites identified as engaging in disinformation activity. Just a few days after the outbreak of war in Ukraine, on 26 February 2022, the National Centre for Cyber Operations of Military Intelligence (NCKO) requested the blocking of 22 pro-Russian websites directly by internet service providers (ISPs) and other entities connected to the NIX inter-operator node. (Czarnecki, 2023, p. 29).

Another form of education consists of briefs from agencies tasked with combating disinformation to the governing elites, ensuring that their representatives remain alert to the issue. The Czech Security Information Service (BIS) regularly warns government politicians in its reports that Russian propaganda in the Czech Republic will first employ the methods and procedures that proved effective in the Slovak Republic (Czarnecki, 2023, p. 34), i.e. disinformation, discrediting politicians opposed to Russia, and the media.

The fundamental mechanism for combating disinformation is, above all, building trust between society and government agencies responsible for countering and tackling it. In Poland, the Ministry of Digital Affairs and the NASK[3] National Research Institute launched a nationwide public campaign in November 2024 to raise awareness of false content online and to educate citizens on how to verify information and report disinformation (Jak nie dać się trollom? Rusza kampania o dezinformacji Ministerstwa Cyfryzacji i NASK, 2024). It is, however, difficult to expect spectacular results even from such a campaign (three radio spots and three television spots) when Poles do not trust either politicians or state institutions. During a roundtable held in November 2024 by the Polish Press Agency (PAP) and NASK concerning electoral disinformation and its impact on voting outcomes, Magdalena Wilczyńska, Director of the Information Security in Cyberspace Division at NASK, stated that Poles assume that disinformation and harmful content on the Internet are simply a part of public debate, and therefore see no point in reporting it or informing experts dealing with disinformation (NASK: dezinformacja realnie wpływa na wyniki wyborów, 2024). This is a significant problem, not only in Poland, but also in other NATO countries, where disinformation, including from Russia, is a significant problem in building trust in the state, which is a key factor for combating it.

Legal instruments aimed at penalising such activities can also serve as tools for combating disinformation spread by foreign intelligence services. In Poland, the Act of 17 August 2023 amending the Criminal Code and certain other acts, added § 9 to Article 130 (the crime of espionage), which reads as follows:

> *Whoever, taking part in the activities of a foreign intelligence service or acting on its behalf, spreads disinformation consisting in disseminating false or misleading information with the aim of causing serious disruption to the political system or economy of the Republic of Poland, of an allied state, or of an international organisation of which the Republic of Poland is a member, or with the aim of inducing a public authority of the Republic of Poland, an al-*

lied state, or an international organisation of which the Republic of Poland is a member, to take or refrain from specific action, shall be subject to a penalty of imprisonment for no less than 8 years.[4] (Ustawa z dnia 17 sierpnia 2023 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw, 2023) (Hoc, 2023, pp. 138–139).

However, the concept of disinformation is not defined in the Criminal Code. In light of the provisions introduced in Article 130 § 9, only activities involving the dissemination of false or misleading information as part of participation in the activities of a foreign intelligence service, or acting on its behalf, are punishable. This is a directional offence, as the perpetrator's objective must be to cause serious disruption to the political system or economy of the Republic of Poland, an allied state, or an international organisation of which Poland is a member, or to induce such authorities to take or refrain from specific actions.

There is serious doubt whether this provision could be applied to ordinary social media users who share false or satirical messages or conspiracy theories. Criminal liability under Article 130 § 9 of the Criminal Code is subject to the same strictures as other types of espionage, namely the requirement for law enforcement to demonstrate a conscious connection between the "disinformant" and a foreign intelligence service; for example, by proving that the dissemination of content was the result of a task assigned by a foreign intelligence agency. According to many legal experts, including Stanisław Hoc, in order to even begin examining the purpose and nature of a message suspected of being disinformation, which in itself is a difficult task, it is first necessary to satisfy the primary and most important component of the crime: demonstrating that conscious cooperation with a foreign intelligence service actually took place (Hoc, 2023, p. 138). So far there have been no court cases in Poland involving this amendment to art. 130 of the Penal Code.

Recommendations for tackling disinformation

Disinformation, as a cheap, easily accessible tool that exploits the internet, has become ubiquitous. It is used to construct various narratives, including for the purposes of state actors. State agencies, such as intelligence services, are often employed to carry out these operations. This is an extremely complex mechanism affecting both NATO as an institution and its individual members. In their publicly available reports, many of NATO

member states' intelligence agencies emphasise that the scope and intensity of disinformation have increased with the outbreak of war in Ukraine. This has been accompanied by a range of disinformation targeting NATO member states, addressing both the credibility and military effectiveness of the alliance, as well as the intentions and political and military capabilities of its members. The solidarity of NATO members with Ukraine is constantly subjected to disinformation aimed at weakening it, ultimately seeking to bring about an end to the conflict on terms favourable to Russia. Poland is also a target of such operations, which are directed at destabilising society, provoking social unrest, and undermining the country's international position and credibility.

The counter-disinformation measures described above, despite involving joint initiatives, do not constitute permanent, legally regulated NATO policy. Institutions studying disinformation in Poland, including the INFO OPS Polska Foundation, call for closer cooperation between the European Parliament and NATO in terms of knowledge sharing and training on disinformation. NATO possesses extensive experience in analysing the methods employed in this area by Russia, Belarus, and China. (Obce manipulacje informacyjne i ingerencja zewnętrzna (FIMI). Zagrożenia i przeciwdziałanie w Polsce za okres od 2014 do 2024 r., 2024, p. 32). One valuable initiative would be to create a platform for the exchange of information concerning all recorded cases of disinformation and its sources in each of the allied countries.

In the context of disinformation spread by foreign intelligence services, which in Poland is strongly associated with Russian intelligence, it is also worth highlighting a certain ineffectiveness of legal provisions intended to enable the prosecution of individuals responsible for its spreading. This is indicated in the Situational Reports of the Polish Government Plenipotentiary for Information Space Security, Stanisław Żaryn, which are compiled based on data from Polish intelligence services. It should be noted that since the formation of the new government in 2023, such reports, if they are produced, are no longer made publicly available. This is closely related to the gaps in information space protection in Poland identified by the INFO OPS Polska Foundation, including weaknesses in the media system and a lack of education in media literacy. Polish intelligence services, responsible for countering foreign intelligence agencies, including disinformation spread on their behalf, do not engage in any communication with the public. Lacking press officers and absent from social media platforms (with the exception of the Military Counterintelligence Service (AW), which has accounts on Facebook and LinkedIn, and the Internal Security Agency (ABW), which has

an account on LinkedIn) they have no direct contact with citizens. Polish intelligence services also do not build their public image or "communication channels" through traditional media (such as television or radio stations; for example, the NASK public awareness campaign is promoted via these channels) or even billboards. As a result, they lose the opportunity to gather information and respond actively to emerging threats.

The Internal Security Agency (ABW) and the Military Counterintelligence Service (SKW), which in Poland hold counterintelligence responsibilities, i.e. are tasked with identifying, detecting, and prosecuting espionage or cooperation with foreign intelligence, continue to face personnel challenges (staff shortages and recruitment difficulties), structural issues (the ongoing reconstruction of regional structures and delegations over several months), and financial constraints. In this context, it is significant that disinformation and its channels of propagation are relatively new phenomena, requiring the acquisition and development of new competencies in both cyberspace and social dimensions. Active collaboration with non-governmental and research institutions specialising in both identifying disinformation and developing tools to operate in cyberspace or the infosphere is also desirable. However, this is not a model of cooperation routinely practised by Polish intelligence services.

Examples of disinformation directed against NATO member states, as well as the mechanisms of combating it, presented in the article, do not exhaust the issue of experiences in this area common to Poland and selected NATO countries. They are only a contribution to further academic discussions on the subject.

NOTES

[1] The text was created as part of a project carried out by the Institute of Turkish Studies as part of the competition of the Minister of Foreign Affairs of the Republic of Poland "Dyplomacja Publiczna 2024–2025 – wymiar europejski i przeciwdziałanie dezinformacji."

[2] KAPO zapisywane jest również jako KaPo oraz tłumaczone jako Policyjny Urząd Bezpieczeństwa. Podlega on Ministerstwu Spraw Wewnętrznych, a powołany został 1 marca 1991 r. jako oddział Policji. Od 18 lipca 1993 r. działa jako samodzielna instytucja, zaś od 1 marca 2001 r. na mocy odrębnego prawa o urzędach bezpieczeństwa został przekształcony z urzędu policyjnego w urząd bezpieczeństwa. (Kaitsepolitseiamet, ESTONIA, 2025)

[3] NASK stands for *Naukowa i Akademicka Sieć Komputerowa* – Scientific and Academic Computer Network (translator's note).

[4] Pol. *Kto, biorąc udział w działalności obcego wywiadu albo działając na jego rzecz, prowadzi dezinformację, polegającą na rozpowszechnianiu nieprawdziwych lub wprowadzających w błąd informacji mając na celu wywołanie poważnych zakłóceń w ustroju lub gospodarce Rzeczypospolitej Polskiej, państwa sojuszniczego lub organizacji międzynarodowej,*

której członkiem jest Rzeczypospolita Polska albo skłonienie organu władzy publicznej Rzeczypospolitej Polskiej, państwa sojuszniczego lub organizacji międzynarodowej, której członkiem jest Rzeczypospolita Polska, do podjęcia lub zaniechania określonych czynności, podlega karze pozbawienia wolności na czas nie krótszy niż 8 lat.

REFERENCES

NASK: dezinformacja realnie wpływa na wyniki wyborów, 2024. https://www.pap.pl/mediaroom/nask-dezinformacja-realnie-wplywa-na-wyniki-wyborow. [Online].

Aleksandrowicz, T. R., 2013. Służby specjalne w strategicznym zapewnieniu bezpieczeństwa państwa. W: J. Gryz, red. *Strategia bezpieczeństwa narodowego Polski.* Warszawa: Wydawnictwo Naukowe PWN.

Aleksandrowicz, T. R., 2021. *Zagrożenie dla bezpieczeństwa informacyjnego państwa w ujęciu systemowym. Budowanie zdolności defensywnych i ofensywnych w infosferze.* Warszawa: Difin.

Annual Review 2022–2023 Estonian Internal Security Service, 2023. https://kapo.ee/sites/default/files/content_page_attachments/annual-review-2023-2024.pdf. [Online].

Bąkowicz, K., 2023. *Dezinformacja. Instrukcja obsługi, Warszawa 2023.* Warszawa: CeDeWu.

Bezpečnostní informační služba, Zpráva o činnosti za 2018, 2018. https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2018-vz-cz.pdf.pdf. [Online].

CSIS Public Report 2023, 2023. https://www.canada.ca/content/dam/csis-scrs/documents/publications/Public_Report_2023-eng-DIGITAL.pdf. [Online].

Czarnecki, S., 2023. Dezinformacja w Republice Czeskiej. In: *Dezinformacja w Republice Czeskiej i Republice Słowackiej w obliczu wojny rosyjsko-ukraińskiej.* Lublin: Instytut Europy Środkowej.

Dezinformacja przeciwko Polsce, 2023. https://www.gov.pl/web/sluzby-specjalne/dezinformacja-przeciwko-polsce2. [Online].

Hoc, S., 2002. Sytuacja organizacyjno-prawna polskich służb specjalnych. *Wojskowy Przegląd Prawniczy*, Issue 3.

Hoc, S., 2023. Szpiegostwo w znowelizowanym Kodeksie karnym. *Nowa Kodyfikacja Prawa Karnego*, Issue 67, pp. 119–143.

Informacja, 28.03.2024, 2024. https://www.abw.gov.pl/pl/informacje/2471,Komunikat.html. [Online].

International Security and Estonia, 2023. https://www.valisluureamet.ee/doc/raport/2023-en.pdf. [Online].

Jak nie dać się trollom? Rusza kampania o dezinformacji Ministerstwa Cyfryzacji i NASK, 2024. https://www.gov.pl/web/cyfryzacja/jak-nie-dac-sie-trollom-rusza-kampania-o-dezinformacji-ministerstwa-cyfryzacji-i-nask. [Online].

Justice Department Leads Efforts Among Federal, International, and Private Sector Partners to Disrupt Covert Russian Government-Operated Social Media Bot Farm, 2024. https://www.justice.gov/archives/opa/pr/justice-department-leads-efforts-among-federal-international-and-private-sector-partners. [Online].

Kaitsepolitseiamet, ESTONIA, 2025. https://www.antykorupcja.gov.pl/ak/instytucje-antykorupcy/inne-agendy-rzadowe-i-i/na-swiecie/1714,ESTONIA-Kaitsepolitseiamet.html. [Online].

Komunikat ABW z dn. 12 października 2023 r., 2023. https://www.abw.gov.pl/pl/informacje/2398,Sledztwo-w-sprawie-dezinformacji.html. [Online].

Meldunek sytuacyjny 02/09/2023, 2023. https://www.gov.pl/web/sluzby-specjalne/dezinformacja-przeciwko-polsce2. [Online].

Meldunek sytuacyjny 03/06/2023, 2023. https://www.gov.pl/web/sluzby-specjalne/dezinformacja-przeciwko-polsce2. [Online].

Meldunek sytuacyjny 07/04/2023, 2023. https://www.gov.pl/web/sluzby-specjalne/dezinformacja-przeciwko-polsce2. [Online].

Meldunek sytuacyjny 09/02/2023, 2023. https://www.gov.pl/web/sluzby-specjalne/dezinformacja-przeciwko-polsce2. [Online].

Meldunek sytuacyjny 17/03/2023, 2023. https://www.gov.pl/web/sluzby-specjalne/dezinformacja-przeciwko-polsce2, 16 XII 2024. [Online].

Meldunek sytuacyjny 17/06/2023, 2023. https://www.gov.pl/web/sluzby-specjalne/dezinformacja-przeciwko-polsce2. [Online].

Meldunek sytuacyjny 20/05/2023, 2023. https://www.gov.pl/web/sluzby-specjalne/dezinformacja-przeciwko-polsce2. [Online].

Meldunek sytuacyjny 21/04/2023, 2023. https://www.gov.pl/web/sluzby-specjalne/dezinformacja-przeciwko-polsce2. [Online].

Meldunek sytuacyjny 23/02/2023, 2023. https://www.gov.pl/web/sluzby-specjalne/dezinformacja-przeciwko-polsce2. [Online].

Meldunek sytuacyjny 26/05/2023, 2023. https://www.gov.pl/web/sluzby-specjalne/dezinformacja-przeciwko-polsce2. [Online].

Meldunek sytuacyjny 27/08/2023, 2023. https://www.gov.pl/web/sluzby-specjalne/dezinformacja-przeciwko-polsce2 .[Online].

Meldunek sytuacyjny 28/04/2023, 2023. https://www.gov.pl/web/sluzby-specjalne/dezinformacja-przeciwko-polsce2. [Online].

Minkina, M. i Gałek, B., 2015. *Kłamstwo i podstęp we współczesnym świecie.* Warszawa: Oficyna Wydawnicza Rytm.

NATO Climate Change and Security Impact Assessment, 2024. https://www.nato.int/nato_static_fl2014/assets/pdf/2024/7/pdf/240709-Climate-Security-Impact.pdf. [Online].

NATO's approach to counter information, 2025. https://www.nato.int/cps/en/natohq/topics_219728.htm. [Online].

Noelle-Neumann, E., 2004. *Spirala milczenia.* Poznań: Zysk i S-ka.

Obce manipulacje informacyjne i ingerencja zewnętrzna (FIMI). Zagrożenia i przeciwdziałanie w Polsce za okres od 2014 do 2024 r., 2024. https://infoops.pl/obce-manipulacje-informacyjne-i-ingerencja-zewnetrzna-fimi-zagrozenia-i-przeciw. [Online].

Słownik terminów i definicji NATO, 2024. https://wcnjik.wp.mil.pl/u/AAP6PL.pdf. [Online].

Sprawozdanie Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa za 2023 rok, 2023. https://www.gov.pl/web/cyfryzacja/krajobraz-cyberprzestrzeni. [Online].

Umożliwiali prowadzenie dezinformacji. Zatrzymała ich ABW, 2021. https://www.gov.pl/web/sluzby-specjalne/umozliwiali-prowadzenie-dezinformacji-zatrzymala-ich-abw. [Online].

Ustawa z dnia 17 sierpnia 2023 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw, 2023. *Dz.U. 2023, poz. 1834.*

Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, Dz.U. 2025, poz. 902.

Zalewski, S., 2005. *Służby specjalne w państwie demokratycznym.* Warszawa: Akademia Obrony Narodowej.