Internal Security Review
2026, no. 34, pp. 363–387

https://doi.org/10.4467/20801335PBW.26.017.23379

ARTICLE

Hybrid attacks against the Republic of Poland conducted and coordinated by the Russian Federation and their link to the war in Ukraine

AGATA RYTEL

Warsaw School of Economics

https://orcid.org/0009-0008-1506-1822

Abstract

The aim of this article is to describe attacks and hybrid activities from the Russian Federation against the Republic of Poland from June 2021 to the end of 2024. They are presented with a distinction between attacks against the integrity of the Polish border with Belarus, attacks carried out in Polish cyberspace, and disinformation attacks in the Polish information space. The thesis adopted in the article assumes that these actions were directly related to the war in Ukraine and were intentional interference by Russia and Belarus. The literature on the theory of hybrid warfare and the actions carried out by the Russian Federation and Belarus, perceived as part of hybrid warfare, was analysed. Furthermore, information related to hostile actions against the Republic of Poland, made available by Polish state institutions and teams set up to respond to computer incidents, was analysed.

Keywords

hybrid attacks, hybrid warfare, illegal migration, cyberspace, disinformation

Introduction

The geopolitical situation in Europe and worldwide has changed significantly in recent years, partly due to the increasingly overt imperialist ambitions of the Russian Federation. Current events (the war in Ukraine, hybrid attacks against Poland) are linked to the dynamic development of network technologies and the unprecedented impact of cyberspace on the functioning of states and societies. The development of tools offered by cyberspace is conducive to hybrid activities. Russia is gradually developing methods of conducting hostile activities against other states that remain below the threshold of war. These include irregular activities on the territory of the attacked state and activities involving attacks on its cyberspace and information sphere. The RF's goals are to weaken the state, cause disorganisation, undermine trust in the government and public institutions, and polarise society. An intensification of Russian hybrid attacks on Poland was observed with the outbreak of full-scale war in Ukraine. A sudden increase in the number of attacks on Polish cyberspace and the infosphere occurred with the migration crisis on the Polish-Belarusian border in 2021.

There are few publications in the literature on subject that compare various methods of hybrid attacks carried out by Russia against Poland. Given the pace of technological development and the impact of cyberspace and the infosphere (often used for hybrid attacks) on the functioning of the state and society, raising awareness of the subject of research seems fundamental.

The aim of this article[1] is to describe hybrid attacks and activities carried out by the RF between June 2021 and December 2024, which threatened the national security and cyberspace of the Republic of Poland. The thesis adopted in the article assumes that the attacks on the integrity of Poland's border carried out by the RF with the help of Belarus were related to the war in Ukraine and that the hybrid activities targeting Poland before and during the war were intentional, systematic interference by Russia and Belarus. In order to achieve the research objectives, methods such as analysis, synthesis and inference were used. The literature on the subject, reports prepared by Polish state institutions, as well as official information related to hostile actions against the Republic of Poland, made available by teams set up to respond to computer incidents, were analysed.

[1] The article is based on a thesis entitled *Hybrid attacks conducted and coordinated by the Russian Federation against the Republic of Poland in the context of the war in Ukraine*, written under the supervision of Jerzy Surma, Associate Professor at the Warsaw School of Economics (SGH). The thesis was defended in 2025 as part of postgraduate studies at SGH in Warsaw in cybersecurity management.

The theory of hybrid warfare

Hybrid warfare is a combination of warfare in the classical sense and other types of activities. These can occur independently, in parallel, or in quick succession. This pattern creates a wide range of possibilities for the attacker and, consequently, generates a large set of threats that the attacked party must contend with.

It should be noted that definitions of hybrid warfare differ between Western countries and the RF. The Russian theory was developed in opposition to the theory developed in the United States and Western Europe. The transfer of terminology to Russian soil is intended to emphasise its 'defensive' nature[2]. The most frequently cited Western theorist of hybrid warfare is Frank G. Hoffman from the United States, who notes that wars of this kind are not new, but are different each time[3]. According to him, this type of conflict is characterised by (…) *convergence* (…) *physical and psychological, the kinetic and nonkinetic, and combatants and noncombatants* (…), *military force and the interagency community, of states and nonstate actors, and of the capabilities they are armed with*[4]. The concept of convergence in the context of Hoffman's theory can be understood as the simultaneous occurrence and interpenetration of military and non-military elements in actions characteristic of hybrid warfare.

Olga Wasiuta and Sergiusz Wasiuta present other characteristics of hybrid warfare identified in American theory. These are:

- a combination of conventional warfare, irregular warfare, information warfare and cyber warfare,
- carrying out attacks using various methods and tools,
- using a combination of weapons and irregular warfare (guerrilla warfare, terrorism, crime),
- a complex, dynamic and flexible battlefield,
- rapid response and adaptation of participants to the dynamics of the conflict,
- use of modern technologies, actions and methods of mobilisation[5].

Valery Gerasimov is considered to be the leading Russian researcher of hybrid warfare theory. Although he does not use the term hybrid warfare in his deliberations,

---

[2] J. Darczewska, *Anatomia rosyjskiej wojny informacyjnej. Operacja Krymska – studium przypadku* (Eng. The anatomy of Russian information warfare. Operation Crimea – a case study), Warszawa 2014, p. 11.

[3] F.G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars*, Arlington 2007, p. 8.

[4] F.G. Hoffman, *Hybrid Warfare and Challenges*, "Joint Force Quarterly" 2009, no. 52, p. 34.

[5] O. Wasiuta, S. Wasiuta, *Wojna hybrydowa Rosji przeciwko Ukrainie* (Eng. Russia's hybrid war against Ukraine), Kraków 2017, pp. 56–57.

he points to elements characteristic of this phenomenon, i.e. the need to use various political, economic and humanitarian instruments in modern conflicts as well as to combine them with the manipulation of the sentiments of the community inhabiting the adversary's territory. These actions are to be supported by non-military means such as information warfare and special forces operations. In the later stages of the conflict, the use of armed forces is permitted, but in the form of peacekeeping or humanitarian missions[6].

Andrzej Krzak also described other definitions of hybrid warfare found in Russian literature on the subject. According to one of the theories he cited, hybrid warfare is characterised by a multitude of different types of activities, conducted in a conventional (classical) and irregular manner, with the support of non-military segments. According to another Russian theory, hybrid warfare is characterised in international relations by comprehensive and methodical military, political, economic and social influence. In yet another Russian approach to hybrid warfare, this time in a military-political context, it is the use of various military and political tactics, as well as socio-economic destabilisation activities, on the territory of a potential adversary[7].

The RF is turning its hybrid warfare doctrine into real actions against other countries, and in connection with the outbreak of war in Ukraine, especially against Poland. Russian actions bearing the hallmarks of hybrid warfare against Poland can be divided into three key areas: the migration crisis, cyber attacks and disinformation campaigns. These actions are coordinated in terms of timing, the tools used, the entities carrying them out and their objectives. Despite Russia's efforts to shift the blame and responsibility for the attacks away from itself, Polish services and experts[8] have in many cases unequivocally attributed responsibility to Russia and Belarus as well as revealed their motivations and hostile intentions.

---

[6] A. Krzak, *Wars of the future in Russian – hybrid, sociological and psychological war in view of the Ukrainian conflict*, "Przegląd Bezpieczeństwa Wewnętrznego" 2018, no. 18, pp. 233–234.

[7] Ibid.

[8] See in more detail: *Hybrydowa agresja Białorusi na UE* (Eng. Belarus' hybrid aggression against the EU), Serwis Rzeczypospolitej Polskiej, 9 XI 2021, https://www.gov.pl/web/sluzby-specjalne/hybrydowa-agresja-bialorusi-na-ue [accessed: 3 VI 2025]; M. Marek, *Wojna informacyjna Federacji Rosyjskiej przeciwko Ukrainie, Polsce i NATO* (Eng. The Russian Federation's information war against Ukraine, Poland and NATO), Warszawa 2025.

Attacks on the integrity of the Polish border with Belarus

The migration crisis that Poland has been facing since 2021 is part of hybrid activities carried out by Russia with the help of Belarus. It is organised and managed by Alexander Lukashenka's regime, which uses migrants as a tool of political pressure. Attacks targeting the integrity of the Polish border, supported by hostile disinformation activities, are aimed at destabilising the security of Poland and the European Union, exerting political pressure, polarising and antagonising society, and creating opportunities for terrorists and other criminals to enter the EU[9].

Migrants, who are the subject of hybrid activities coordinated by the regimes of Belarus and Russia, attempt to cross the Polish border from Belarus illegally on a daily basis[10]. The Polish-Belarusian border is also part of the eastern border of the EU, the Schengen area and NATO. Lithuania was the first country affected by the migration crisis caused by Russia and Belarus, having to deal with it as early as July and August 2021. The data cited below indicate that at the same time as the migration crisis on the Polish-Belarusian border, the Border Guard recorded an increased number of attempts by third-country nationals to cross the Polish-Lithuanian border illegally[11].

According to the spokesperson for the special services coordinator, almost the entire state apparatus of the Belarusian regime is involved in organising activities related to the next stage of the hybrid war. The organisational scheme of the illegal migration route begins with special travel agencies issuing invitations to migrants and the Belarusian Ministry of Foreign Affairs issuing 'tourist' visas. The migrants then arrive in Belarus on Belarusian state airlines, which have created new connections specifically for this purpose. From the airports, migrants are transported to the border with Poland[12]. There, Belarusian services support the actions of migrants who attempt to cross the border by force, attack Polish border guards and destroy infrastructure[13].

---

[9] *Hybrydowy atak na Polskę* (Eng. Hybrid attack on Poland), Serwis Rzeczypospolitej Polskiej, 9 VIII 2022, https://www.gov.pl/web/sluzby-specjalne/hybrydowy-atak-na-polske [accessed: 30 V 2025].

[10] *Wojna Federacji Rosyjskiej z Zachodem* (Eng. The Russian Federation's war with the West), M. Banasik (sci. ed.), Warszawa 2022, p. 126.

[11] *Bezpieczeństwo Europy Środkowo-Wschodniej. Perspektywa narodowa i międzynarodowa* (Eng. Security in Central and Eastern Europe. National and international perspectives), W. Śmiałek, Ł. Kominek, O. Balogh (sci. eds.), Poznań 2022, pp. 293–294.

[12] *Hybrydowa agresja Białorusi na UE…*

[13] *Bezpieczeństwo i zagrożenia hybrydowe* (Eng. Security and hybrid threats), M. Banasiak, A. Rogozińska (sci. eds.), Warszawa 2022, p. 22.

The escalation of aggressive actions by migrants on the Polish-Belarusian border took place on 8 November 2021. They attempted to force their way onto the Polish side, destroying the fence with the active support of the Belarusian services[14]. Another aggressive attempt at illegal mass border crossing by foreigners took place on 16 November at the border crossing in Kuźnica.

The tension at the border was further heightened by various provocations used by officers of the Belarusian regime. They verbally assaulted Polish officers and soldiers, threw stones at them, tried to stun them with firecrackers, and blind them with spotlights and lasers. Provocations involving Belarusian services firing shots at the border, uniformed persons with long weapons crossing it, and even aiming weapons at Polish soldiers and officers on duty at the border were commonplace[15].

In 2021, the Border Guard recorded 2869 foreigners – the citizens of third countries (from outside the EU) who were detained for crossing the state border in violation of regulations (hereinafter: pgpwp) or attempting pgpwp on the border with Belarus. This represents an increase of 1164% compared to 2020 (227 foreigners were recorded). Among those detained, the largest groups were citizens of Iraq, Afghanistan, Syria, Somalia, Russia and Belarus. During the same period, the Border Guard registered 320 third-country nationals apprehended/detected for pgpwp or attempted pgpwp on the border with Lithuania. This represents an increase of 158% compared to 2020 (124 foreigners were recorded). Most of the apprehended persons came from Iraq and Syria[16].

In 2022, the Border Guard recorded 586 third-country nationals detained for pgpwp or attempted pgpwp on the section of the border with Belarus. This is a decrease of 80% compared to 2021. Most of the apprehended/detected persons were citizens of Iraq, Syria, Iran, Afghanistan and Belarus. During the same period, the Border Guard recorded 726 third-country nationals apprehended/detected for pgpwp or attempted pgpwp on the border with Lithuania. This represents an increase of 127% compared to 2021. The largest number of persons apprehended/detected came from Iraq, Afghanistan, Iran and Syria[17].

In 2023, the Border Guard recorded 562 third-country nationals detained for pgpwp or attempted pgpwp on the border with Belarus, which represents

[14] *Wielowymiarowość konfliktów kulturowych we współczesnym świecie* (Eng. The multidimensionality of cultural conflicts in the modern world), W. Śmiałek (sci. ed.), Poznań 2024, p. 186.

[15] Ibid., p. 187.

[16] Statystyki SG – styczeń–grudzień 2021 (Eng. SG statistics – January–December 2021), https://www.strazgraniczna.pl/pl/granica/statystyki-sg/2206,Statystyki-SG.html [accessed: 30 V 2025].

[17] Statystyki SG – styczeń–grudzień 2022 (Eng. SG statistics – January–December 2022), https://www.strazgraniczna.pl/pl/granica/statystyki-sg/2206,Statystyki-SG.html [accessed: 30 V 2025].

a 4% decrease compared to 2022. Most of the apprehended/detected persons came from Afghanistan, Belarus and Syria. On the border with Lithuania, the Border Guard recorded 727 third-country nationals apprehended/detected for pgpwp or attempted pgpwp. This represents an increase of 0.1% compared to 2022. The largest number of persons apprehended/detected came from Syria, Afghanistan, Iran and India[18].

In 2024, the Border Guard recorded 2582 third-country nationals detained for pgpwp or attempted pgpwp on the border with Belarus. This represents an increase of 359% compared to 2023. Most of the apprehended/detected persons were citizens of Ethiopia, Eritrea, Somalia, Syria, Yemen, Sudan and Afghanistan. During the same period, the Border Guard registered 432 third-country nationals who were apprehended/detected for pgpwp or attempted pgpwp on the border with Lithuania. Compared to 2023, this is a decrease of 41%. The largest number of persons apprehended/detected came from Afghanistan, Moldova and Belarus[19].

It should be noted that the statistics cited refer to migrants who were actually apprehended/detected. The number of attempts to cross the Polish-Belarusian and Polish-Lithuanian borders is significantly higher. According to the Podlaski Border Guard Regional Unit and the Nadbużański Border Guard Regional Unit, in 2021 alone, 39 697 attempts to cross the border illegally outside border crossings were recorded on the border with Belarus. This is over 300 times more attempts than in 2020[20]. In 2024, according to the Podlaski Border Guard Regional Unit, nearly 30 000 attempts to illegally cross the Polish-Belarusian border were recorded. The migrants came from 52 countries, mainly Ethiopia, Eritrea and Somalia. A total of 346 organisers of illegal border crossings and their accomplices were also detained, including 316 people on the border with Belarus and 30 on the border with Lithuania. The majority of those detained were citizens of Ukraine, Poland and Belarus[21].

---

[18] Statystyki SG – styczeń–grudzień 2023 (Eng. SG statistics – January–December 2023), https://www.strazgraniczna.pl/pl/granica/statystyki-sg/2206,Statystyki-SG.html [accessed: 30 V 2025].

[19] Statystyki SG – styczeń–grudzień 2024 (Eng. SG statistics – January–December 2024), https://www.strazgraniczna.pl/pl/granica/statystyki-sg/2206,Statystyki-SG.html [accessed: 30 V 2025].

[20] E. Szczepańska, *Nielegalne przekroczenia granicy z Białorusią* (Eng. Illegal border crossings from Belarus), Straż Graniczna, 12 I 2022, https://www.strazgraniczna.pl/pl/aktualnosci/9689,Nielegalne-przekroczenia-granicy-z-Bialorusia-w-2021-r.html [accessed: 3 VI 2025].

[21] K. Zdanowicz, *Nielegalna migracja w Podlaskim Oddziale Straży Granicznej – podsumowanie* (Eng. Illegal migration in the Podlaski Border Guard Regional Unit – summary), 21 I 2025, https://www.podlaski.strazgraniczna.pl/pod/aktualnosci/64039,Nielegalna-migracja-w-Podlaskim-Oddziale-Strazy-Granicznej-podsumowanie.html?search=858959366 [accessed: 3 VI 2025].

The migration crisis on the Polish-Belarusian border is an example of deliberate and organised hybrid actions in which Russia, with the help of the Belarusian regime, is using migrants as a tool for political blackmail. The state apparatus of Lukashenka's regime not only organises and controls the migration route, but also conducts coordinated provocative and disinformation activities aimed at blaming Poland for the crisis and causing divisions within Polish society and on the international stage. Such operations demonstrate how Russia exploits contemporary threats in its hybrid activities to destabilise security and order in Poland and Europe.

Attacks in cyberspace

The intensity of Russian cyberattacks targeting Poland increased significantly just before and after Russia's invasion of Ukraine, as confirmed by the statistics presented below. The attacks are part of a broader hybrid strategy by the Kremlin aimed at destabilising the situation in Poland, putting pressure on the Polish authorities and causing chaos and uncertainty among the population. Pro-Russian hacker groups target state institutions as well as the private sector, the media and citizens. They use advanced methods such as distributed denial of service (DDoS) attacks, ransomware, phishing and impersonating official government websites. Some of these activities are a direct response to Poland's support for Ukraine and to political decisions by the Polish authorities that are unfavourable to the RF. In modern conflicts, cyberspace has become an important battlefield, and its effective protection requires constant monitoring and rapid response.

APT (advanced persistent threats) attacks carried out by groups of the same name are particularly dangerous. These are advanced, long-term attacks characteristic of this type of cybercriminal groups operating on behalf of governments. APT groups attack to obtain strategic information, conduct cyber espionage, disrupt the functioning of the attacked country, and influence its politics and economy. Financial support from governments provides cybercriminals with access to advanced resources and technologies that facilitate long-term and complex cyberattacks[22]. Pro-Russian groups constitute a significant segment of this environment[23].

[22] *Krajobraz cyberzagrożeń w polskim sektorze finansowym 2025* (Eng. The cyber threat landscape in the Polish financial sector in 2025), https://cebrf.knf.gov.pl/images/GTL_2025_FINAL.pdf, p. 6 [accessed: 10 VI 2025].

[23] Ibid., p. 14.

According to information provided by the Government Plenipotentiary for the Security of Information Space of the Republic of Poland, incidents in cyberspace are typical retaliatory actions by Russia in response to actions taken by other countries that are unfavourable to the RF[24]. Hacker groups using DDoS attacks, ransomware, phishing, and fake websites impersonating existing services are linked to the Kremlin. Entities in strategic sectors, such as energy and defence, are particularly at risk. The attacks are consistent with the objectives of hybrid operations, which are designed to cause destabilisation, intimidation and chaos. Every cyberattack has specific consequences – political, financial and social[25].

The *Act of 5 July 2018 on the national cybersecurity system* established three computer security incident response teams in Poland, namely CSIRT GOV, CSIRT NASK and CSIRT MON. Due to the subject matter of the reports on the state of Polish cybersecurity published by these teams, the author of the article analysed the reports of CSIRT GOV and CERT Polska (operating within the structure of CSIRT NASK) for the years 2021–2024 as well as the reports for the years 2021–2022 prepared by the CSIRT KNF, which is a computer security incident response team in the Polish financial sector, were also analysed[26].

Since 2010, the CSIRT GOV team (led by the Head of the Internal Security Agency) has been publishing annual reports on the state of cyber security in Poland[27]. The largest increase in the number of reports of potential incidents, and consequently the increase in the number of confirmed incidents, was recorded in the third and fourth quarters of 2021. The largest number of reports concerned, in order: critical infrastructure, institutions, offices, ministries, services and the military, and other sectors[28]. In its 2021 report, the CSIRT GOV team reported a more than threefold increase in the number of reports of potential ICT security incidents compared to the previous year. The activity of sponsored APT groups was also noted, particularly in the context of critical infrastructure and public

[24] *Rosyjskie cyberataki* (Eng. Russian cyberattacks), Serwis Rzeczypospolitej Polskiej, 29 XII 2022, https://www.gov.pl/web/sluzby-specjalne/rosyjskie-cyberataki [accessed: 5 VI 2025].

[25] Ibid.

[26] *Centrum Edukacji dla Bezpieczeństwa Rynku Finansowego* (Eng. Education Centre for Financial Market Security), Urząd Komisji Nadzoru Finansowego, https://cebrf.knf.gov.pl [accessed: 10 VI 2025].

[27] Raporty o stanie bezpieczeństwa cyberprzestrzeni RP (Eng. Reports on the state of cybersecurity in Poland), Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego, https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi [accessed: 5 VI 2025].

[28] CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2021 roku* (Eng. Report on the state of cyberspace security in Poland in 2021), Warszawa 2022, p. 14.

administration[29]. In turn, the CERT Polska team reported an 182% increase in the number of incidents handled in 2021 compared to the previous year[30].

In its 2021 report analysing cyber security threats to the financial market in Poland, CSIRT KNF also noted that the largest increase in the number of reported dangerous websites occurred in the third and fourth quarters of 2021[31].

On the gov.pl website, in the section on cybersecurity, from 2022 onwards, more and more articles began to appear on the threats posed by fraud and disinformation, and in 2023, articles began to be published that explicitly mentioned Russian cyberattacks[32].

The CSIRT GOV report for 2022 devoted an entire chapter for the first time to analysing the activities of APT groups whose activity in Polish cyberspace was related to the war in Ukraine[33]. It highlighted previously unreported threats and activities on such a large scale, including an increasing number of social engineering campaigns and DDoS attacks, which were primarily targeted at public services provided on the internet. The CSIRT GOV team classified the largest number of incidents in 2022 in the following categories: vulnerability, social engineering and unavailability. The vulnerability category recorded the highest number of incidents due to the introduction of the CHARLIE-CRP alert level in February 2022, which resulted in an increase in the number of identified events that could have compromised the security of Poland's ICT infrastructure.

The social engineering campaigns recorded by CSIRT GOV in 2022 included phishing campaigns, website spoofing and impersonation (often of government administration websites or government systems). Their intensity remained high, and the targets were mass recipients and representatives of selected entities. These activities were primarily aimed at gaining unauthorised access to the resources of the attacked entity by obtaining authentication data. In addition, the attacks were

[29] Ibid., p. 64.

[30] CERT Polska, *Raport roczny z działalności CERT Polska 2021. Krajobraz bezpieczeństwa polskiego internetu* (Eng. Annual report on the activities of CERT Polska 2021. The security landscape of the Polish internet), Warszawa 2022, p. 12.

[31] CSIRT KNF, *Podsumowanie Roku w CSIRT KNF 2021. Opis wybranych ataków* (Eng. Summary of the Year at CSIRT KNF 2021. Description of selected attacks), https://cebrf.knf.gov.pl/images/Komunikaty/Raporty/Pdf/RaportCSIRTKNF_76474.pdf [accessed: 8 VI 2025].

[32] Baza wiedzy – cyberbezpieczeństwo (Eng. Knowledge base – cybersecurity), Serwis Rzeczypospolitej Polskiej, https://www.gov.pl/web/baza-wiedzy/aktualnosci [accessed: 8 VI 2025].

[33] CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2022 roku* (Eng. Report on the state of cyberspace security in Poland in 2022), Warszawa 2023, p. 56.

aimed at distributing malware and gaining access to IT systems in order to carry out further cybercriminal activities[34].

In the category of unavailability, a significant increase in the number of DDoS attacks (826 incidents, compared to 310 in the previous year) targeting Polish public administration websites and critical infrastructure has been recorded since February 2022. These attacks were carried out by hacktivist groups, including Killnet, NoName057(16), the People's Cyber Army. The CSIRT GOV team indicated that in 2022, the component most vulnerable to attacks in cyberspace was Poland's critical infrastructure[35]. It also confirmed that Poland's actions on behalf of Ukraine in the war with Russia have significantly increased the level of threat in Polish cyberspace.

In its annual report on activities in 2022, the CERT Polska team devotes an entire chapter to the impact of the war in Ukraine on Polish cybersecurity. In retrospect, it has been confirmed that Russia's military operations are supported by the activities of hackers and hacktivist groups, as well as the spread of disinformation. Russia had already been conducting these intensified activities in cyberspace in the months preceding the conventional war in Ukraine. The events in Polish cyberspace that CERT Polska, like CSIRT GOV, directly links to the war in Ukraine include massive DDoS attacks on government websites and the websites of important economic entities, as well as phishing campaigns using the war theme and appearing mainly on social media. The report states that the attacks are intended to destabilise the internal situation in countries that support Ukraine. Examples of DDoS attacks carried out by Russian hacktivists are given. Their frequent ineffectiveness and use primarily to spread propaganda and disinformation are highlighted. It also lists campaigns that use the appearance of well-known websites and government websites, as well as the theme of war. The frauds included, among others, fake Facebook login panels, fake fundraisers, Nigerian scams, and fake investments[36].

In its 2022 report, CSIRT KNF also devoted a chapter to threats and recommendations regarding DDoS attacks and hacktivist activities in the context of the war in Ukraine. The team reported that DDoS attacks were the most numerous in 2022. They had a certain impact on the financial sector in Poland. The high availability, ease of use, relatively low cost and effectiveness of this type of criminal method were emphasised. The possibility of almost anyone carrying

[34] Ibid., p. 30.

[35] Ibid., pp. 13–17.

[36] CERT Polska, *Raport roczny z działalności CERT Polska 2022. Krajobraz bezpieczeństwa polskiego internetu* (Eng. Annual report on the activities of CERT Polska 2022. The security landscape of the Polish internet), Warszawa 2023, pp. 93–100.

out (planning and directing attacks) or participating (sharing their resources) in an attack was also indicated. The CSIRT GOV team also noted that the targets of pro-Russian cybercriminal groups depend on the political actions of countries which, in the opinion of hacktivists, are hostile to Russia or favourable to Ukraine[37].

The CSIRT GOV report for 2023 includes information that Poland continued to face heightened cyber threats related to the armed conflict in Ukraine this year. Based on an assessment of APT group activity in 2023, it was concluded that these attacks were largely a continuation of those recorded in 2022. The main targets of the attacks remained state institutions and critical infrastructure, especially in the energy and transport sectors. Two types of criminal activity dominated: DDoS attacks – used by pro-Russian groups to disrupt websites and public services, as well as social engineering campaigns – aimed at phishing for data, infecting systems with malware and destabilising political processes. These activities were intensified in connection with parliamentary elections in Poland. The report shows that in 2023, Poland was a key target of Russian hybrid operations combining cyberattacks with information warfare[38].

In its 2023 report, the CERT Polska team presented an analysis of APT group activities. Since the start of the war in Ukraine, there has been a significant increase in their activity, which in 2023 was primarily aimed at disrupting the continuity of operations of Polish entities in the transport and logistics sector[39]. It has been noted that these groups are linked to the RF and/or Belarus[40].

In its 2024 activity report, the CSIRT GOV team reported that Poland continued to experience an elevated level of cyber threats, including social engineering, attempts to exploit vulnerabilities, DDoS attacks, and the publication of leaked data, also carried out by sponsored hacktivist groups. In 2024, there were events of particular importance from a security perspective, namely local elections, European Parliament elections, and the 33rd Summer Olympic Games in Paris. The incidents of 2024 described in the report confirmed that cybercriminals and state actors are interested in any entities whose attack would also affect national security. The report also stated that cyberattacks are a hybrid threat and an element of modern conflicts in which hostile actions are conducted below the threshold

[37] CSIRT KNF, *Cyberzagrożenia w sektorze finansowym 2022* (Eng. Cyber threats in the financial sector 2022), https://cebrf.knf.gov.pl/images/Cyberzagroenia_w_sektorze_finansowym_2022.pdf [accessed: 8 VI 2025].

[38] CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2023 roku* (Eng. Report on the state of cyberspace security in Poland in 2023), Warszawa 2024, pp. 4–6.

[39] CERT Polska, *Raport roczny z działalności CERT Polska 2023* (Eng. Annual report on the activities of CERT Polska 2023), Warszawa 2024, p. 34.

[40] Ibid.

of war[41]. Particular attention was paid to the threat of attacks on supply chains, which were defined as attacks targeting a trusted external service provider essential to that chain. This has broadened the potential area of attack on key infrastructure sectors in Poland[42]. It has been confirmed that attacks by APT groups, motivated by ideology, politics and finance, continue to pose the greatest threat to government administration and critical infrastructure. In 2024, these groups focused on continuing their activities from 2022–2023, and as before, this activity was supported by propaganda campaigns designed to demonstrate the effectiveness and potential of cyberattacks. It was noted that 2024 was characterised by an increase in the volume of cybercriminal groups, which was caused by a growth in the number of financially motivated groups and increasing access to AI-assisted tools. The main actors mentioned were APT28 group (also known as Fancy Bear), followed by groups APT29 (also known as Cozy Bear), UNC1151 (also known as Ghostwriter), APT15, and DaVinci[43].

In its 2024 activity report, the CERT Polska team presented an observation similar to that of the CSIRT GOV team regarding the activity of APT groups, mainly associated with the RF and Belarus. It reported that these groups were pursuing intelligence and propaganda objectives, and that most of these activities consisted of attempts to obtain authentication data for e-mail accounts, distribution of malware, and attacks on industrial systems. It also drew attention to the practice of attacking not only public institutions and large enterprises, but also smaller entities that are links in supply chains. The CERT Polska team identified UNC1151, APT28 and APT29 as the most active of the observed APT groups[44].

It should be noted that all teams presented similar conclusions in their analyses regarding trends, main types of threats and sectors most vulnerable to cyber attacks in Poland. These are:

- a significant increase in the number of reports and confirmed incidents on the network since 2021 compared to previous years, noticeable several months before Russia's aggression against Ukraine in 2022,
- intensified and dynamic activity of cybercriminal groups linked to the RF and Belarus,

[41] CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2024 roku* (Eng. Report on the state of cyberspace security in Poland in 2024), Warszawa 2025, pp. 5–6.

[42] Ibid., p. 113.

[43] Ibid., pp. 54–56.

[44] CERT Polska, *Raport roczny 2024 z działalności CERT Polska. Krajobraz bezpieczeństwa polskiego internetu* (Eng. Annual Report on the activities of CERT Polska 2024. The security landscape of the Polish internet), Warszawa 2025, p. 33.

- the most common types of attacks were DDoS attacks and social engineering campaigns,
- one of the intentions of the attacks was to cause widespread disruption to the functioning of the state,
- the targets of cyberattacks were primarily government administration, public institutions and critical infrastructure entities,
- a characteristic activity of APT groups is the promotion of their activities on social media,
- an increase in the number of attacks targeting smaller entities that are links in supply chains.

In May 2025, the American equivalent of Polish CSIRT teams, i.e. the Cybersecurity and Infrastructure Security Agency, published a report on the specific threat currently faced by Eastern European entities, including Polish ones, which are links in supply chains. This threat is posed by the APT28 group, which has been mentioned repeatedly by Polish teams. As emphasised by the American source, it is identified with the Russian Main Intelligence Directorate (GRU) and the Russian military unit 26165[45].

Cyberspace has become a key arena for hybrid activities, including both technical attacks and accompanying information campaigns aimed at destabilising the state and exerting social and political pressure. Russian cyberattacks are part of a hybrid strategy, often responding to actions unfavourable to Russia and forming an integral part of the war with Ukraine.

Disinformation in the Polish information space

Propaganda and disinformation activities on the part of Russia have been observed since at least the days of the Soviet Union, but President Vladimir Putin's rule has made Russia one of the most active actors in the information sphere, including cyberspace, on the international political scene[46]. The comprehensive activities carried out by the RF are referred to as information warfare and include coordinated propaganda and disinformation campaigns in cyberspace[47]. Information warfare is seen as one of the most important elements of Russia's international competition strategy,

[45] *Russian GRU Targeting Western Logistics Entities and Technology Companies*, CISA, 21 V 2025, https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-141a [accessed: 10 VI 2025].

[46] *Informacja czynnikiem warunkującym bezpieczeństwo. Kontekst rosyjski* (Eng. Information as a factor determining security. The Russian context), M. Banasik (sci. ed.), Warszawa 2021, p. 7.

[47] Ibid.

enabling it to achieve its political goals. Cyberspace, on the other hand, enables the RF to conduct activities within the framework of this information warfare[48].

Jerzy Surma emphasises the special role played by social media in information warfare. He draws attention to the consequences for national security of the easy and cheap possibility of publishing and exchanging information. These features of social media make them both a place and a tool for waging information wars, the aim of which is to manage information in such a way as to influence the behaviour of society and shape it according to the will of the attacker.

Information warfare is conducted in an organised manner, using both overt activities, such as propaganda and manipulation of information, and covert activities, including the fabrication of information for the purpose of disinformation. He cited the RF as an example of a state that systematically conducts activities that bear the hallmarks of information warfare as part of hybrid warfare[49].

The following objectives can be attributed to hostile actions of this type:

- disruption of the value system (breakdown of social bonds, isolation of individuals or groups, distrust of public institutions),
- attacks on important facilities (critical infrastructure, places of worship and international symbols),
- creation and exploitation of opinion leaders (shaping perceptions by influential individuals and/or those with the ability to influence large audiences)[50].

The literature on the subject emphasises the multifaceted nature of Russian campaigns in the information sphere, as well as their strategic importance. The information war they wage involves processes that target the cognitive sphere of human beings and shape people's attitudes in line with the attacker's expectations[51].

Since 24 February 2022, Russians have been undermining the image of the Republic of Poland both in their own and external infosphere. This activity included, among other things, developing Polish-language channels on the Telegram platform (where hacktivist groups shared, for example, false information about attacks on Polish facilities for propaganda purposes[52]), the activities of so-called

---

48 Ibid., p. 8.

49 J. Surma, *Cyfryzacja życia w erze Big Data. Człowiek. Biznes. Państwo* (Eng. The digitisation of life in the era of Big Data. People. Business. The State), Warszawa 2017, p. 90.

50 *Odporność państwa, społeczeństwa i gospodarki na zagrożenia* (Eng. Resilience of the state, society and economy to threats), M. Piotrowska-Trybull, K. Górska-Rożej (sci. eds.), Warszawa 2024, pp. 331–332.

51 *Informacja czynnikiem warunkującym bezpieczeństwo*…, p. 50.

52 CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2022 roku*…, pp. 25–28.

troll and bot accounts, and the noticeable activity of groups involved in spreading Russian narrative. Disinformation materials and narratives present on Russian channels on Telegram, including Polish-language ones, were then shared on other channels in the Polish segment of social networks. The newly formed Polish Anti-War Movement and campaigns with political overtones, such as 'Stop the Ukrainisation of Poland' and 'This is not our war', also contributed to the achievement of Russian information objectives. In addition, the Belarusian side exposed Polish citizens who had emigrated to Belarus and Russia and started pro-Russian disinformation activities. They spread Russian propaganda and disinformation on social media[53].

The Telegram platform was founded by Russian citizens in 2013. In 2021, its Polish-language segment expanded. Two events in 2021, for which Russia is likely responsible, contributed to its popularity in Poland.

The first was the publication on Telegram of data obtained after an attack on the e-mail accounts of Polish politicians[54]. One of them was Minister Michał Dworczyk. Information from his e-mail account began appearing on the Telegram channel on 4 June. Experts say that Russia or Belarus, which cooperates with it, is responsible for these actions[55]. The attack is part of a campaign called 'Ghostwriter,' which aims to obtain data and sensitive information for Russian special services and spread Russian disinformation[56]. As part of this campaign, webmail accounts and social media accounts belonging to public figures from Central and Eastern European countries, mainly Poland, are being attacked. Criminals are attempting to take over information resources for the purposes of Russian disinformation[57].

The second event was the migration crisis on the Polish-Belarusian border in Poland in 2021. Recordings and propaganda messages were disseminated to the Polish infosphere via Telegram (and then other social media platforms and the media)[58]. The popularisation of this tool in Poland allowed the Russian-Belarusian narrative to be disseminated[59].

---

53 M. Marek, *Wojna informacyjna Federacji Rosyjskiej*…, pp. 116–117.

54 Ibid., p. 119.

55 *Afera mailowa. Prokuratura postawiła zarzuty, ale to pionki* (Eng. Email scandal. The prosecutor's office has brought charges, but these are just pawns), CyberDefence24, 16 VIII 2024, https://cyberdefence24.pl/polityka-i-prawo/afera-mailowa-prokuratura-postawila-zarzuty-ale-to-pionki [accessed: 11 VI 2025].

56 *Rozwój technik ataku grupy UNC1151/Ghostwriter* (Eng. Development of attack techniques by the UNC1151/Ghostwriter group), Cert.pl, 19 VII 2022, https://cert.pl/posts/2022/07/techniki-unc1151/ [accessed: 23 VI 2025].

57 *Rosyjskie cyberataki*…

58 M. Marek, *Wojna informacyjna Federacji Rosyjskiej*…, p. 119.

59 Ibid., p. 123.

According to Michał Marek, the head of the External Threat Analysis Team at NASK, Russian disinformation focuses on three main narratives: pushing Poland towards war with Russia[60], NATO and the US being responsible for the outbreak of war in Ukraine[61], and Poland being subjected to so-called Ukrainisation[62]. A year after the outbreak of war in Ukraine, the spokesperson for the Polish Ministry of Foreign Affairs posted a comment in which he wrote about an unprecedented increase in the scale of Russian disinformation activity. He noted that Russia was conducting a large-scale disinformation campaign. Its goals were to undermine the values of a free and democratic world, cause chaos, incite hatred, and destabilise the international order. The spokesman pointed out that despite new forms of false narratives, the basic methods of manipulation remain the same. The goal is also the same – to stir up tensions and unrest in the societies under attack. He warned against providing audiences with contradictory information designed to make people unable to distinguish between truth and falsehood. This would allow even the most absurd versions of events to be believed[63].

In January 2025, a report was published by the disinformation team of the Commission for the Investigation of Russian and Belarusian Influence on the Internal Security and Interests of the Republic of Poland in 2004–2024. It drew attention to the theory of the Russian information warfare strategy, which captures the essence and nature of activities carried out in the Polish infosphere. Content falsified to varying degrees appears in traditional media, social media and online platforms. The report pointed to the Russian news agency Sputnik, which had a Polish version of its website, and the content published on it was shared by fabricated information environments and then by social media accounts[64]. It was also found that with the outbreak of war in Ukraine in 2022, Russian propaganda began to promote a narrative about the defencelessness of Western countries (including Poland) and the weakness of their armies and authorities. The aim was

[60] Ibid., p. 131.

[61] Ibid., p. 140.

[62] Ibid., p. 146.

[63] *O rosyjskiej dezinformacji: rok od pełnoskalowej inwazji na Ukrainę – komentarz Rzecznika Prasowego MSZ* (Eng. On Russian disinformation: one year since the full-scale invasion of Ukraine – commentary by the Spokesperson for the Ministry of Foreign Affairs), Serwis Rzeczypospolitej Polskiej, 23 II 2023, https://www.gov.pl/web/dyplomacja/o-rosyjskiej-dezinformacji-rok-od-pelnoskalowej-inwazji-na-ukraine--komentarz-rzecznika-prasowego-msz [accessed: 14 VI 2025].

[64] Komisja do spraw badania wpływów rosyjskich i białoruskich na bezpieczeństwo wewnętrzne i interesy Rzeczypospolitej Polskiej w latach 2004–2024 (Eng. The Commission for the Investigation of Russian and Belarusian Influence on the Internal Security and Interests of the Republic of Poland in 2004–2024), *Raport Zespołu ds. Dezinformacji*, Warszawa 2025, p. 5.

to convince the audience that the state did not provide them with security and that it was not worth defending in the event of a threat[65]. The experts who compiled this report drew attention to the objectives of Russian disinformation and propaganda, namely the polarisation of society and the erosion of trust in the state, as well as in science, the media and fellow citizens[66].

The scale of Russian disinformation activities is also reflected in the situation reports published on the gov.pl website. In 2023, 31 reports were published describing disinformation activities carried out by Russia and Belarus against Poland. They concerned false accusations against Poland, including brutal treatment of migrants at the border and plans for aggression against Ukraine. These reports emphasised that these activities were aimed at causing social divisions and undermining trust in Polish authorities and institutions, and were also part of an information war aimed at destabilising Poland and the region[67].

The scale of disinformation in 2023 was also revealed by the Government Centre for Security (RCB). As part of the DisInfo Radar project, the RCB published 57 infographics presenting topics covered by Russian and Belarusian disinformation. They included information on false Russian persuasion and narratives, untrue theses, manipulations, and websites observed in 2023[68]. Warnings about the disinformation campaign were issued in particular in October 2023, when parliamentary elections were held in Poland. The threats to the security of the electoral process were listed, and information was provided about an ongoing information campaign suggesting that a coup d'état was being prepared in Poland and that the army would be used against the population[69].

Polish computer incident response teams have also highlighted Russian disinformation campaigns in their annual reports since 2021. In its 2021 activity report, the CSIRT GOV team reported on the activities of APT groups that were attributed with spreading disinformation. One example given was operation 'Ghostwriter', which is attributed to the UNC1151 group[70].

---

65 Ibid., p. 19.

66 Ibid., p. 20.

67 Dezinformacja przeciwko Polsce, meldunki sytuacyjne, Służby specjalne (Eng. Disinformation against Poland, situation reports, Special services), Serwis Rzeczypospolitej Polskiej, https://www.gov.pl/web/sluzby-specjalne/dezinformacja-przeciwko-polsce2 [accessed: 14 VI 2025].

68 Disinfo Radar, Rządowe Centrum Bezpieczeństwa, https://www.gov.pl/web/rcb/disinfo-radar [accessed: 14 VI 2025].

69 Ibid.

70 CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2021 roku*…, p. 27.

In its 2022 activity report, the CSIRT GOV team reported on the identification of incidents that indicated a context of disinformation. An example given was an attack in September 2022 involving the posting of anti-Ukrainian content and propaganda graphics on the website of the Office of Rail Transport. The CSIRT GOV team also reported the identification of a practice involving the registration of websites impersonating official government domains, which indicated the possibility of their use for social engineering attacks, including disinformation[71]. In its report on activities in 2022, the CERT Polska team reported on the disinformation activities of pro-Russian cybercriminal groups. It was found that a characteristic feature of these groups is the spread of disinformation[72].

This phenomenon was also described in the CSIRT GOV activity report for 2023. The team drew attention to the parliamentary elections, which prompted an intensification of activities by hacktivist groups conducting disinformation attacks using various means of communication, including e-mails and text messages. It attributed responsibility for these attacks to, among others, the UNC1151 group[73].

Similar observations were described by the CERT Polska team in its 2023 activity report. It also identified UNC1151 as the most active APT group and pointed to its links with the Belarusian government and Russian special services. The targets were mainly from the political and military circles, but there were also people who could have indirect links to Russia or Belarus, such as lawyers, sworn Russian translators, Orthodox priests, NGO employees and journalists. The motivations for these actions were identified as the theft of information for intelligence purposes and the conduct of disinformation campaigns. In 2023, the team observed disinformation campaigns related to the terrorist threat in Poland, the collection of information about refugees, military recruitment, and the lack of potassium iodide in pharmacies. In the assessment of CERT Polska, the campaigns were aimed at spreading uncertainty and divisions in society. It was noted that after the parliamentary elections, the activity of the UNC1151 group decreased significantly[74].

In its 2024 activity report, the CSIRT GOV team once again drew attention to local government elections and European Parliament elections, which were vulnerable to hostile disinformation operations conducted in cyberspace. Another event associated with a disinformation incident was the 33rd Summer Olympic Games in Paris. In August 2024, the pro-Russian hacktivist groups Beregini and Zarya, acting

[71] CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2022 roku*…, p. 31.

[72] CERT Polska, *Raport roczny z działalności CERT Polska 2022*…, p. 93.

[73] CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2023 roku*…, p. 6.

[74] CERT Polska, *Raport roczny z działalności CERT Polska 2023*…, p. 93.

in concert, stole documents from the IT systems of the Polish Anti-Doping Agency and published them in a modified form in order to discredit Polish athletes[75]. As in previous years, the team observed the activities of the UNC1151 group, which this time was conducting a campaign targeting users of the most popular email providers – Gmail, Interia, Wirtualna Polska, Onet, and o2. The criminals obtained data from mailboxes by impersonating mail administrators and persuading users to log in using a fake login panel[76]. Another serious incident attributed to sponsored cybercriminal groups was the attack on the Polish Press Agency in May 2024. False information about military mobilisation in Poland was posted twice on its official website[77].

In its 2024 activity report, the CERT Polska team, like the CSIRT GOV team, discussed a disinformation campaign targeting the Polish Anti-Doping Agency. In addition, it described a disinformation campaign related to the Steadfast Defender 2024 and Dragon-24 military exercises, concerning an allegedly drunk driver of a military truck. The team emphasised that the disinformation content that appeared in the Polish infosphere in 2024 referred to many socio-political events[78].

Summary

An analysis of information concerning the migration crisis and attacks in cyberspace and the information sphere in Poland allows us to conclude that representatives of Polish government bodies, uniformed services, including special services, as well as specialists involved in detecting and preventing cyber attacks, have no doubt about the specific nature and character of Russian actions directed against Poland. They conclude that Russia's aggressive actions are part of a hybrid war closely linked to the attack on Ukraine. The Russian strategy is characterised by the gradual, planned weakening of its adversary by conducting activities on many levels of the state's functioning. It is precisely such activities that are supposed to be most effective.

The data analysis contained in this article proves the validity of the thesis. The attacks on the integrity of the Republic of Poland carried out by the RF were directly related to the war in Ukraine. Research of source materials conducted using analysis, synthesis and inference allows us to conclude that Russia, in cooperation with Belarus, is responsible for the hybrid attacks carried out against Poland since 2021.

---

[75] CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2024 roku*…, p. 6.

[76] Ibid., p. 69.

[77] Ibid., p. 78.

[78] CERT Polska, *Raport roczny 2024 z działalności CERT Polska*…, p. 35.

Russian hybrid activities are characterised by the blurring of the line between military and civilian areas. Russia uses civilians to achieve its goals. Russian-Belarusian hybrid attacks target areas that may be important for Poland's security. Coordinated attacks in multiple areas simultaneously are intended to increase their severity. It is therefore essential to conduct crisis response exercises covering not only the military sphere but also the civilian sphere, as well as joint cross-sectoral exercises.

Bibliography

Bezpieczeństwo Europy Środkowo-Wschodniej. Perspektywa narodowa i międzynarodowa (Eng. Security in Central and Eastern Europe. National and international perspectives), W. Śmiałek, Ł. Kominek, O. Balogh (sci. eds.), Poznań 2022.

Bezpieczeństwo i zagrożenia hybrydowe (Eng. Security and hybrid threats), M. Banasik, A. Rogozińska (sci. eds.), Warszawa 2022.

Darczewska J., *Anatomia rosyjskiej wojny informacyjnej. Operacja Krymska – studium przypadku* (Eng. The anatomy of Russian information warfare. Operation Crimea – a case study), Warszawa 2014.

Hoffman F.G., *Conflict in the 21st Century: The Rise of Hybrid Wars*, Arlington 2007.

Hoffman F.G., *Hybrid Warfare and Challenges*, "Joint Force Quarterly" 2009, no. 52, pp. 34–39.

Informacja czynnikiem warunkującym bezpieczeństwo. Kontekst rosyjski (Eng. Information as a factor determining security. The Russian context), M. Banasik (sci. ed.), Warszawa 2021.

Krzak A., *Wars of the future in Russian – hybrid, sociological and psychological war in view of the Ukrainian conflict*, "Przegląd Bezpieczeństwa Wewnętrznego" 2018, no. 18, pp. 221–243.

Marek M., *Wojna informacyjna Federacji Rosyjskiej przeciwko Ukrainie, Polsce i NATO* (Eng. The Russian Federation's information war against Ukraine, Poland and NATO), Warszawa 2025.

Odporność państwa, społeczeństwa i gospodarki na zagrożenia (Eng. Resilience of the state, society and economy to threats), M. Piotrowska-Trybull, K. Górska-Rożej (sci. eds.), Warszawa 2024.

Surma J., *Cyfryzacja życia w erze Big Data. Człowiek. Biznes. Państwo* (Eng. The digitisation of life in the era of Big Data. People. Business. The State), Warszawa 2017.

Wasiuta O., Wasiuta S., *Wojna hybrydowa Rosji przeciwko Ukrainie* (Eng. Russia's hybrid war against Ukraine), Kraków 2017.

Wielowymiarowość konfliktów kulturowych we współczesnym świecie (Eng. The multidimensionality of cultural conflicts in the contemporary world), W. Śmiałek (sci. ed.), Poznań 2024.

Wojna Federacji Rosyjskiej z Zachodem (Eng. The Russian Federation's war with the West), M. Banasik (sci. ed.), Warszawa 2022.

Internet sources

Afera mailowa. Prokuratura postawiła zarzuty, ale to pionki (Eng. Email scandal. The prosecutor's office has brought charges, but these are just pawns), CyberDefence24, 16 VIII 2024, https://cyberdefence24.pl/polityka-i-prawo/afera-mailowa-prokuratura-postawila-zarzuty-ale-to-pionki [accessed: 11 VI 2025].

Baza wiedzy – cyberbezpieczeństwo (Eng. Knowledge base – cybersecurity), Serwis Rzeczypospolitej Polskiej, https://www.gov.pl/web/baza-wiedzy/aktualnosci [accessed: 8 VI 2025].

Centrum Edukacji dla Bezpieczeństwa Rynku Finansowego (Eng. Education Centre for Financial Market Security), Urząd Komisji Nadzoru Finansowego, https://cebrf.knf.gov.pl [accessed: 10 VI 2025].

Dezinformacja przeciwko Polsce, meldunki sytuacyjne, Służby specjalne (Eng. Disinformation against Poland, situation reports, Special services), Serwis Rzeczypospolitej Polskiej, https://www.gov.pl/web/sluzby-specjalne/dezinformacja-przeciwko-polsce2 [accessed: 14 VI 2025].

Disinfo Radar, Rządowe Centrum Bezpieczeństwa, https://www.gov.pl/web/rcb/disinfo-radar [accessed: 14 VI 2025].

Hybrydowa agresja Białorusi na UE (Eng. Belarus' hybrid aggression against the EU), Serwis Rzeczypospolitej Polskiej, 9 XI 2021, https://www.gov.pl/web/sluzby-specjalne/hybrydowa-agresja-bialorusi-na-ue [accessed: 3 VI 2025].

Hybrydowy atak na Polskę (Eng. Hybrid attack on Poland), Serwis Rzeczypospolitej Polskiej, 9 VIII 2022, https://www.gov.pl/web/sluzby-specjalne/hybrydowy-atak-na-polske [accessed: 30 V 2025].

Krajobraz cyberzagrożeń w polskim sektorze finansowym 2025 (Eng. The cyber threat landscape in the Polish financial sector in 2025), https://cebrf.knf.gov.pl/images/GTL_2025_FINAL.pdf [accessed: 10 VI 2025].

O rosyjskiej dezinformacji: rok od pełnoskalowej inwazji na Ukrainę – komentarz Rzecznika Prasowego MSZ (Eng. On Russian disinformation: one year since the full-scale invasion of Ukraine – commentary by the Spokesperson for the Ministry of Foreign Affairs), Serwis Rzeczypospolitej Polskiej, 23 II 2023, https://www.gov.pl/web/dyplomacja/o-rosyjskiej-dezinformacji-rok-od-pelnoskalowej-inwazji-na-ukraine--komentarz-rzecznika-prasowego-msz [accessed: 14 VI 2025].

Raporty o stanie bezpieczeństwa cyberprzestrzeni RP (Eng. Reports on the state of cybersecurity in Poland), Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego, https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi [accessed: 5 VI 2025].

Rosyjskie cyberataki (Eng. Russian cyberattacks), Serwis Rzeczypospolitej Polskiej, 29 XII 2022, https://www.gov.pl/web/sluzby-specjalne/rosyjskie-cyberataki [accessed: 11 VI 2025].

Rozwój technik ataku grupy UNC1151/Ghostwriter (Eng. Development of attack techniques by the UNC1151/Ghostwriter group), Cert.pl, 19 VII 2022, https://cert.pl/posts/2022/07/techniki-unc1151/ [accessed: 23 VI 2025].

Russian GRU Targeting Western Logistics Entities and Technology Companies, CISA, 21 V 2025, https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-141a [accessed: 10 VI 2025].

Statystyki SG – styczeń–grudzień 2021 (Eng. SG statistics – January–December 2021), https://www.strazgraniczna.pl/pl/granica/statystyki-sg/2206,Statystyki-SG.html [accessed: 30 V 2025].

Statystyki SG – styczeń–grudzień 2022 (Eng. SG statistics – January–December 2022), https://www.strazgraniczna.pl/pl/granica/statystyki-sg/2206,Statystyki-SG.html [accessed: 30 V 2025].

Statystyki SG – styczeń–grudzień 2023 (Eng. SG statistics – January–December 2023), https://www.strazgraniczna.pl/pl/granica/statystyki-sg/2206,Statystyki-SG.html [accessed: 30 V 2025].

Statystyki SG – styczeń–grudzień 2024 (Eng. SG statistics – January–December 2024), https://www.strazgraniczna.pl/pl/granica/statystyki-sg/2206,Statystyki-SG.html [accessed: 30 V 2025].

Szczepańska E., *Nielegalne przekroczenia granicy z Białorusią* (Eng. Illegal border crossings from Belarus), Straż Graniczna, 12 I 2022, https://www.strazgraniczna.pl/pl/aktualnosci/9689,-Nielegalne-przekroczenia-granicy-z-Bialorusia-w-2021-r.html [accessed: 3 VI 2025].

Zdanowicz K., *Nielegalna migracja w Podlaskim Oddziale Straży Granicznej – podsumowanie* (Eng. Illegal migration in the Podlaski Border Guard Regional Unit – summary), 21 I 2025, https://www.podlaski.strazgraniczna.pl/pod/aktualnosci/64039,Nielegalna-migracja-w-Podlaskim-Oddziale-Strazy-Granicznej-podsumowanie.html?search=858959366 [accessed: 3 VI 2025].

Legal acts

Act of 5 July 2018 on the national cybersecurity system (consolidated text, Journal of Laws of 2026, item 20).

Other documents

CERT Polska, *Raport roczny 2024 z działalności CERT Polska. Krajobraz bezpieczeństwa polskiego internetu* (Eng. Annual Report on the activities of CERT Polska 2024. The security landscape of the Polish internet), Warszawa 2025.

CERT Polska, *Raport roczny z działalności CERT Polska 2021. Krajobraz bezpieczeństwa polskiego internetu* (Eng. Annual report on the activities of CERT Polska 2021. The security landscape of the Polish internet), Warszawa 2022.

CERT Polska, *Raport roczny z działalności CERT Polska 2022. Krajobraz bezpieczeństwa polskiego internetu* (Eng. Annual report on the activities of CERT Polska 2022. The security landscape of the Polish internet), Warszawa 2023.

CERT Polska, *Raport roczny z działalności CERT Polska 2023* (Eng. Annual report on the activities of CERT Polska 2023), Warszawa 2024.

CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2021 roku* (Eng. Report on the state of cyberspace security in Poland in 2021), Warszawa 2022.

CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2022 roku* (Eng. Report on the state of cyberspace security in Poland in 2022), Warszawa 2023.

CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2023 roku* (Eng. Report on the state of cyberspace security in Poland in 2023), Warszawa 2024.

CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2024 roku* (Eng. Report on the state of cyberspace security in Poland in 2024), Warszawa 2025.

CSIRT KNF, *Cyberzagrożenia w sektorze finansowym 2022* (Eng. Cyber threats in the financial sector 2022), https://cebrf.knf.gov.pl/images/Cyberzagroenia_w_sektorze_finansowym_2022.pdf [accessed: 8 VI 2025].

CSIRT KNF, *Podsumowanie Roku w CSIRT KNF 2021. Opis wybranych ataków* (Eng. Summary of the Year at CSIRT KNF 2021. Description of selected attacks), https://cebrf.knf.gov.pl/images/Komunikaty/Raporty/Pdf/RaportCSIRTKNF_76474.pdf [accessed: 8 VI 2025].

Komisja do spraw badania wpływów rosyjskich i białoruskich na bezpieczeństwo wewnętrzne i interesy Rzeczypospolitej Polskiej w latach 2004–2024 (Eng. The Commission for the Investigation of Russian and Belarusian Influence on the Internal Security and Interests of the Republic of Poland in 2004–2024), *Raport Zespołu ds. Dezinformacji*, Warszawa 2025.

Agata Rytel

Graduate of postgraduate studies in cybersecurity management at the Warsaw School of Economics.

Contact: agatakalota0@gmail.com