Terrorism – Studies, Analyses, Prevention, 2025, no. 8: 537–550

https://doi.org/10.4467/27204383TER.25.064.23051

From phishing to sabotage – the evolution of cyber threats to Poland. Conclusions from CSIRT GOV report for 2024

Monika Stodolnik

Independent author

https://orcid.org/0009-0000-5319-7968

Cyberspace, which is nowadays an arena of international competition, is undergoing dynamic changes, and recent years have demonstrated its importance in the context of state non-military activities. It enables operations of an intelligence, sabotage, disinformation nature, as well as influence operations. In this reality, cybersecurity should be an integral part of national resilience – alongside military, energy or economic security.

Poland as a member of international communities and, above all, as an entity actively supporting Ukraine in the face of the aggression from the Russian Federation, is among the countries particularly vulnerable to cyber attacks. *Report on the state of Poland's cybersecurity in 2024*, prepared by the Computer Security Incident Response Team CSIRT GOV operating within the structures of the Internal Security Agency (ABW), provides a valuable source of knowledge about current trends, attack vectors and the level of preparedness of public administration and critical infrastructure operators.

The analysis of the report presented in the article allows conclusions to be drawn not only about the technical aspects of the attacks, but also about the threats to institutions and society in connection with contemporary phenomena in cyber space.

The role of the CSIRT GOV in the national cybersecurity system

The CSIRT GOV team serves as one of three national teams established by the Act on the national cybersecurity system[1], responsible for recognising and detecting of threats to public administration systems and critical infrastructure as well as preventing them. The CSIRT GOV carries out tasks imposed by both the Act on the national cybersecurity system and the Act on the Internal Security Agency and the Foreign Intelligence Agency[2]. It thus combines technical, operational and analytical competences, and is responsible for monitoring the cyberspace of the Republic of Poland, responding to incidents and coordinating activities in the field of its protection.

The CSIRT GOV is an operational element of the national cybersecurity system, directly supporting implementation of state tasks in the area of information protection, counteracting cyber threats, which is a key element of hybrid threats, and ensuring continuity of critical infrastructure operation. Its position within the ABW structure allows for combining ongoing technical analysis of incidents with an assessment of their broader context, including their impact on national security, taking into account the counterintelligence perspective. This assessment also covers the aspect of prevention – for state administration and operators of critical infrastructure.

Cybersecurity context in 2024

Throughout 2024, an elevated CRP alert level was maintained (in January and February – CHARLIE-CRP, and from March onwards – BRAVO-CRP[3] level). This involved maintaining constant readiness to respond to potential

[1] *Act of 5 July 2018 on the national cybersecurity system* (Journal of Laws of 2024, item 1077, as amended).

[2] *Act of 24 May 2002 on the Internal Security Agency and the Foreign Intelligence Agency* (consolidated text, Journal of Laws of 2025, item 902, as amended).

[3] CSIRT GOV, *Report on the state of Poland's cybersecurity in 2024*, https://csirt.gov.pl/download/3/221/RaportostaniebezpieczenstwacyberprzestrzeniRPw2024.pdf, p. 5 [accessed: 1 X 2025].

terrorist activities, in accordance with the Act on anti-terrorist activities[4]. In a broader sense, this means constant readiness to respond to potential incidents of hybrid and cyber intelligence nature, due to the common attack vectors used in all these cases.

In 2024, the CSIRT GOV registered 17 439 reports on potential incidents, of which 3991 were considered to be actual breaches of the security of ICT systems (Figure 1)[5]. Although these figures indicate a decline compared to 2023, the authors of the report point out that this is not so much due to a reduction in the number of threats as to an improvement in the competence and awareness of users as well as the implementation of more effective protection mechanisms in institutions[6].

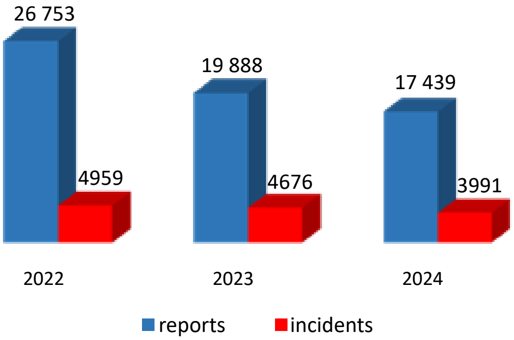

Figure 1. Number of reports and incidents recorded by the CSIRT GOV between 2022 and 2024.

Source: CSIRT GOV, *Report on the state of Poland's cybersecurity in 2024*, https://csirt.gov.pl/download/3/221/RaportostaniebezpieczenstwacyberprzestrzeniRPw2024.pdf, p. 10 [accessed: 1 X 2025].

The above data illustrates the increasing resilience of entities within the competence of the CSIRT GOV. Factors contributing to this increased resilience include:

1) preventing attacks at the network edge, i.e. effectively filtering and blocking intrusion attempts before they reach the right ICT systems. In the case of social engineering attacks using e-mail,

[4] *Act of 10 June 2016 on anti-terrorist activities* (consolidated text, Journal of Laws of 2025, item 194).

[5] CSIRT GOV, *Report on the state of Poland's cybersecurity…*, p. 10.

[6] Ibid.

this means using advanced anti-spam filters and reputation mechanisms on mail gateways; in the case of force attacks – implementing solutions such as IP address blocking (so-called blacklisting) or login attempt limits, and in the case of threats exploiting known vulnerabilities – keeping software up to date and eliminating security gaps;

2) increased awareness among users and administration employees, who are increasingly able to recognise and stop social engineering attempts (e.g. phishing, spearphishing, vishing) at the stage of contact with a message or suspicious link, before interacting with them. This is the result of an increasing number of training courses, warning messages and internal incidents response procedures. In 2024, the CSIRT GOV conducted training courses and workshops for nearly 1900 people, which is almost four times more than in 2023[7];
3) development of internal structures responsible for cybersecurity, such as SOC (Security Operations Center) teams or IT security units in public institutions. This allows for more effective handling of incidents at the local level, without the need to involve the CSIRT GOV each time;
4) strengthening interinstitutional cooperation and coordination, both within the three national CSIRT teams (GOV, MON, NASK) and between public administration and critical infrastructure operators. The exchange of threat intelligence and distribution of indicators of compromise (IoC) enable earlier detection of attack attempts and faster response to incidents. Based on incident reports and analysis of indicators of compromise from a single case, the CSIRT GOV develops warnings and recommendations for its entire area of competence, which helps prevent the spread of threats[8];
5) using security tests and audits as proactive measures that allow for the safe and controlled identification of system vulnerabilities before they are exploited by criminal and cyber offensive groups. Such activities, carried out by units within the structure of a given entity, external companies providing penetration testing services

[7] Ibid.

[8] Ibid., p. 15.

or the CSIRT GOV are an important element of prevention and improving the overall digital resilience of public administration entities and critical infrastructure operators. In 2024, the CSIRT GOV conducted a series of penetration tests in public administration institutions. These included, among other things, an assessment of system configurations, the effectiveness of defence mechanisms and the quality of vulnerability management. The conclusions from these tests were used to develop recommendations for specific entities[9].

Characteristics of cyber offensive activities in the context of cybersecurity in the Republic of Poland

The increase in the competence and capabilities of entities falling within the remit of the CSIRT GOV does not eliminate all threats. The analysis of incidents recorded in 2024 indicates that despite a noticeable improvement in security levels and user awareness, Polish cyberspace remains a place of activity for criminal, intelligence and hacktivist entities[10]. Events resulting from the actions of state-sponsored groups are one of the elements that make up incidents divided by the CSIRT GOV into two categories referred to as 'social engineering' and 'attack'. The first category mainly refers to phishing targeting users of organisations of interest to the actors, while the second concerns attempts and successful incidents of breaching the security of the ICT infrastructure of the attacked entities[11].

In 2024, the activity of state-sponsored groups and pro-Russian hacktivist collectives remained high. International reports place Poland among the leading European countries in terms of the number of socially and politically motivated, sponsored attacks. A report by Microsoft, an IT company, shows that in 2024 Poland was among the top three countries in Europe[12]. In turn, according to analysts from technology company,

[9] Ibid., p. 96.

[10] Ibid., p. 54.

[11] Ibid., pp. 12–13.

[12] *Microsoft Digital Defense Report 2024, The foundations and new frontiers of cybersecurity*, https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Microsoft%20Digital%20Defense%20Report%202024%20%281%29.pdf, p. 13 [accessed: 19 III 2025].

Radware, Poland ranked second among European countries, behind Ukraine, in terms of the number of DDoS attacks[13] initiated by pro-Russian hacktivists[14]. This confirms that Poland, as an active ally of Ukraine and the eastern border of NATO and the European Union, was particularly vulnerable to asymmetric and hybrid actions in a cyberspace.

The CSIRT GOV report points to the predominance of attacks from the Russian direction, particularly those carried out by APT28 group (military unit no. 26165 within the 85th Main Special Service Centre of the General Staff Main Intelligence Directorate GRU[15]) and APT29 group[16] (subordinate to the Foreign Intelligence Service of the Russian Federation)[17]. The cases discussed, recorded in the cyberspace of the Republic of Poland, are also confirmed in the foreign publications cited in the article, which show the broader context of the activities of these groups.

The campaign by APT29 group, also known as Earth Koshchei, using RDP (remote desktop protocol) connection configuration files, was most likely (according to Microsoft analysts' findings based on registered domain names[18]) targeted, among others, at European government entities, particularly foreign and defence ministries, NATO structures, as well as the Ukrainian defence, energy and telecommunications sectors (Figure 2). This clearly fits into the context of the activities of the intelligence service of the state waging war against Ukraine and hybrid activities against NATO

[13] DDoS (distributed denial of service) attack – coordinated overload of system or service resources through a large number of simultaneous requests from different devices, intended to prevent proper operation.

[14] *2024 Global Threat Analysis Report, Executive Summary*, https://www.cisco.com/c/dam/m/en_in/events/security-conclave-2024/radware-threat-report-summary-2024.pdf, p. 9 [accessed: 2 X 2025].

[15] *Działania rosyjskiej służby specjalnej GRU wymierzone w zachodnie podmioty logistyczne oraz przedsiębiorstwa technologiczne* (Eng. Actions by the Russian GRU special service targeting Western logistics entities and technology companies), https://www.gov.pl/attachment/e9e86877-2ba0-478e-be36-f20d68474f37, p. 4 [accessed: 14 X 2025].

[16] APT29, MITRE ATT&CK, https://attack.mitre.org/groups/G0016/ [accessed: 14 X 2025].

[17] CSIRT GOV*, Report on the state of Poland's cybersecurity…*, p. 56.

[18] *Midnight Blizzard conducts large-scale spear-phishing campaign using RDP files*, Microsoft Threat Intelligence, 29 X 2024, https://www.microsoft.com/en-us/security/blog/2024/10/29/midnight-blizzard-conducts-large-scale-spear-phishing-campaign-using-rdp-files/ [accessed: 14 X 2025].

states, and the list of potential recipients of the campaign coincides with those previously recorded[19].

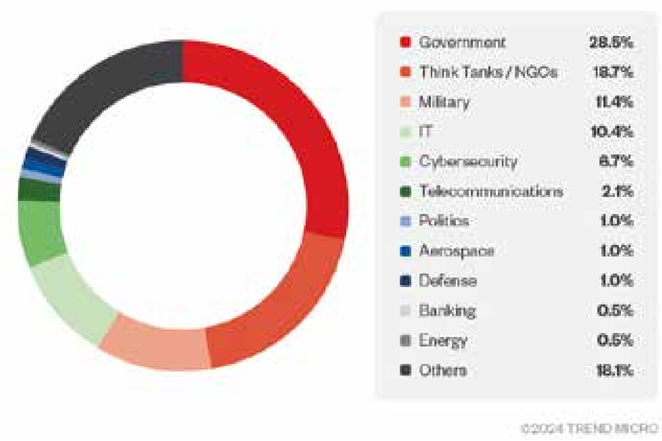

Figure 2. Percentage of domains registered by APT29 group, divided into economic sectors.

Source: *Earth Koshchei Coopts Red Team Tools in Complex RDP Attacks*, Trend Micro, 17 XII 2024, https://www.trendmicro.com/en_us/research/24/l/earth-koshchei.html [accessed: 14 X 2025].

Among the threats posed by APT28 group, social engineering attacks predominated, including those involving the theft of e-mail login details and the infection of workstations with malware designed to steal sensitive information. Attacks exploiting various types of ICT system vulnerabilities were also identified[20]. In the context of ICT, 'vulnerabilities' refer to weaknesses in systems that that an attacker may use to carry out an effective attack[21]. However, it should be emphasised that this term does not refer exclusively to software errors recorded in the CVE (Common Vulnerabilities and Exposures) database, but also includes configuration errors, user behaviour and unintended software features that may be exploited in a manner contrary to their intended purpose[22].

[19] *Threat profile: APT29*, https://blackpointcyber.com/wp-content/uploads/2024/06/Threat-Profile-APT29_Blackpoint-Adversary-Pursuit-Group-APG_2024.pdf, p. 4 [accessed: 2 X 2025].

[20] CSIRT GOV, *Report on the state of Poland's cybersecurity...*, p. 57–66.

[21] *Vulnerability management, Understanding vulnerabilities*, National Cyber Security Centre, https://www.ncsc.gov.uk/collection/vulnerability-management/understanding-vulnerabilities [accessed: 10 X 2025].

[22] Ibid.

For example, a weak point in the system may be the use of simple or repetitive passwords, which is sometimes exploited in brute force attacks on login panels. The lack of filtering of traffic originating from anonymising VPN[23] or TOR[24] networks is also a significant weakness, making it easier for attackers to conceal the source of their activities. The analysed cases also noted the use of vulnerabilities enabling DCSync attacks[25] that allow domain credentials to be obtained[26]. In turn, certain system functions, such as mechanisms for granting permissions to email folders in Microsoft Exchange service, may be used in accordance with their design, but in a malicious manner to escalate privileges or exfiltrate data[27]. Such a broad range of vulnerability means that an organisation's cyber resilience depends not only on keeping its software up to date, but also on proper configuration of the environment, user discipline, and understanding how an adversary may exploit system functions.

The APT28 group used these funds to attack both entities in Poland, and in other countries, including those belonging to NATO. In May 2025, this was reported in a joint document by the services of the United States, the United Kingdom, Germany, the Czech Republic, Poland, Australia, Canada, Denmark, Estonia, France and the Netherlands[28]. This document provides a detailed description of the GRU's activities, as presented by the CSIRT GOV, towards entities carrying out tasks to support Ukraine in the war with Russia, as well as technology companies, and at the same time presents another dimension of the GRU's presence in Western countries and Ukraine, apart from its sabotage activities[29] (Figure 3).

[23] Virtual Private Network – encrypted tunnel service between the user's device and an intermediary server, masking the user's actual IP address and location.

[24] The Onion Router – anonymising network that redirects network traffic through a large number of encrypted nodes.

[25] DCSync attack – technique in which an attacker impersonates Active Directory domain controller and requests data synchronisation, thereby obtaining cryptographic hashes of credentials for all accounts in the domain.

[26] CSIRT GOV, *Report on the state of Poland's cybersecurity…*, p. 65.

[27] Ibid.

[28] *Działania rosyjskiej służby specjalnej GRU…*, p. 7.

[29] A. Jawor, *"Agenci jednorazowego użytku" rosyjskiego GRU. "Tajna" kampania sabotażu w Europie* (Eng. "Disposable agents" of the Russian GRU. "Secret" sabotage campaign in Europe), CyberDefence24, 3 X 2025, https://cyberdefence24.pl/armia-i-sluzby/agenci-jednorazowego-uzytku-rosyjskiego-gru-tajna-kampania-sabotazu-w-europie [accessed: 14 X 2025].

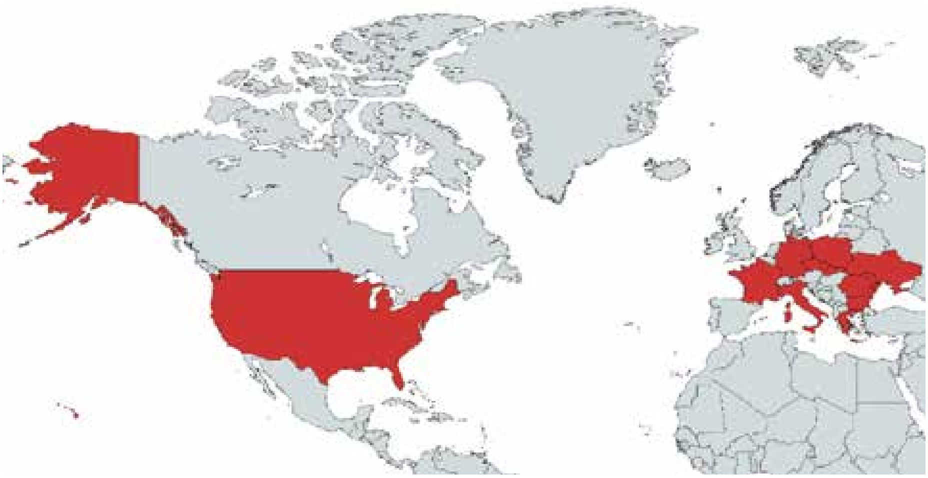

Figure 3. Geographical location of entities targeted by the GRU actions.

Source: *Działania rosyjskiej służby specjalnej GRU wymierzone w zachodnie podmioty logistyczne oraz przedsiębiorstwa technologiczne* (Eng. Actions by the Russian GRU special service targeting Western logistics entities and technology companies), Serwis Rzeczypospolitej Polskiej, https://www.gov.pl/attachment/e9e86877-2ba0-478e-be36-f20d68474f37, p. 7 [accessed: 14 X 2025].

Among the threats analysed by the CSIRT GOV, the activity of groups linked to the People's Republic of China, which in 2024 conducted intelligence operations against the Member States of the European Union, was identified. It focused on gathering information in the following areas: science and technology, energy and public administration. The attacks reported in Poland were carried out by two groups – Volt Typhoon[30] and APT15[31]. Furthermore, the network of TP-Link devices hijacked by Chinese cybercriminals has been identified. It was used to anonymise traffic in attacks on Microsoft services[32]. These activities are part of a long-term strategy to covertly obtain information of great importance to industry and the economy in order to strengthen China's technological potential and competitiveness on the international stage.

Also noteworthy is the activity of entities associated with the Republic of Belarus, which are highly likely to be working in cooperation with

[30] Volt Typhoon – the group attributed to the People's Liberation Army, attacking the critical infrastructure of Western countries in order to conduct intelligence operations.

[31] APT15 – cyber offensive group attributed to China, pursuing China's strategic intelligence objectives.

[32] CSIRT GOV, *Report on the state of Poland's cybersecurity…*, pp. 72–73, 75.

the services of the Russian Federation. In 2024, the activities of UNC1151 group, which conducts two types of activities – disinformation and intelligence, were observed[33]. Its campaigns included phishing messages impersonating login panels for the most popular Polish e-mail services – Interia, Onet, Wirtualna Polska. The aim was to obtain login details, take over accounts and build the infrastructure needed for disinformation campaigns. In order to carry out espionage activities, computers were infected with malware that allowed full control of the devices to be taken over. This was done via email. The group's activity has been observed since at least 2017[34], which indicates the long-term, reconnaissance nature of their activities and their focus on destabilising the state through information warfare.

The report also noted the activities of pro-Russian hacktivist groups: Beregini and Zarya. The groups published manipulated data stolen from the Polish Anti-Doping Agency to undermine the credibility of Polish athletes during the Olympic Games in Paris[35]. These activities are referred to as *hack-and-leak* operations. They combine a cyber attack with information manipulation aimed at influencing public opinion[36].

In the case of industrial infrastructure (Operational Technology/ Industrial Control Systems), the hacktivist activity increasingly involves targets related to public utility installations, such as sewage treatment plants, water supply networks and pumping stations[37]. This is international trend observed in the United States[38], the Netherlands, France[39] and

[33] Ibid., pp. 69–72.

[34] *Ghostwriter Update: Cyber Espionage Group UNC1151 Likely Conducts Ghostwriter Influence Activity*, https://services.google.com/fh/files/misc/ghostwriter_update_report.pdf, p. 8 [accessed: 14 X 2025].

[35] CSIRT GOV*, Report on the state of Poland's cybersecurity…*, p. 6.

[36] S. Palczewski*, Kampanie hack-and-leak. Czy namieszają przed wyborami w Polsce?* (Eng. Hack-and-leak campaigns. Will they stir things up before the elections in Poland?), Demagog, 17 VIII 2023, https://demagog.org.pl/analizy_i_raporty/kampanie-hack-and-leak-czy-namieszaja-przed-wyborami-w-polsce/ [accessed: 13 X 2025].

[37] CSIRT GOV*, Report on the state of Poland's cybersecurity…*, p. 55.

[38] *Defending OT Operations Against Ongoing Pro-Russia Hacktivist Activity*, https://www.cisa.gov/sites/default/files/2024-05/defending-ot-operations-against-ongoing-pro-russia-hacktivist-activity-508c.pdf, p. 1 [accessed: 1 X 2025].

[39] *Cyber Insight, Sector 16 group*, https://www.orangecyberdefense.com/fileadmin/global/CyberIntelligenceBureau/Gangs_Investigations/Sector16/Sector16Group.pdf, p. 10 [accessed: 1 X 2025].

Norway[40]. The CSIRT GOV report does not specify any particular cases, but only points to the intensification of such activities. Among the most active collectives showing the results of attacks carried out on dedicated channels on the Telegram platform, the following should be noted: Cyber Army of Russia Reborn (CARR), Z-Pentest[41], Sector16 and TwoNet[42]. The latter three are part of an alliance operating under the leadership of the OverFlame (Figure 4).

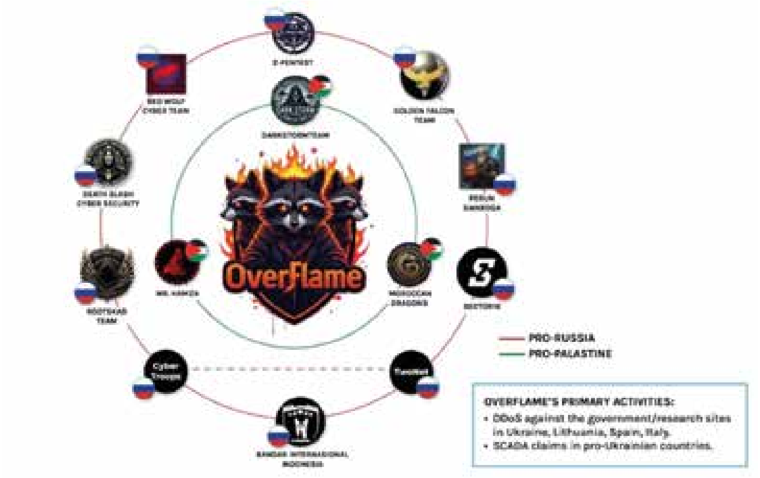
Z-PENTEST
RED WOLF CYBER TEAM
GOLDEN FALCON TEAM
DARKSTORMTEAM
DEATH GLASH CYBER SECURITY
PERUN SVAROGA
OverFlame
MR. HAMZA
MOROCCAN DRAGONS
SECTOR16
ROOTSKAD TEAM
Cyber Troops
TwoNet
BANDAR INTERNASIONAL INDONESIA
PRO-RUSSIA
PRO-PALASTINE
OVERFLAME'S PRIMARY ACTIVITIES:
• DDoS against the government/research sites in Ukraine, Lithuania, Spain, Italy.
• SCADA claims in pro-Ukrainian countries.

Figure 4. Hacktivist groups focused within OverFlame collective.

Source: *Anatomy of a Hacktivist Attack: Russian-Aligned Group Targets OT/ICS*, Forescout, 9 X 2025, https://www.forescout.com/blog/anatomy-of-a-hacktivist-attack-russian-aligned-group-targets-otics/ [accessed: 12 X 2025].

The activity of these collectives is characterised by high dynamics. Channels are frequently deactivated, new groups and alliances as well as conflicts are formed. At the same time, there are many indications that behind many collectives there is a small group of the same people who

[40] M. Bryant, *Russian hackers seized control of Norwegian dam, spy chief says,* The Guardian, 14 VIII 2025, https://www.theguardian.com/world/2025/aug/14/russian-hackers-control-norwegian-dam-norway [accessed: 14 X 2025].

[41] CSIRT GOV, *Report on the state of Poland's cybersecurity...*, p. 74.

[42] *Anatomy of a Hacktivist Attack: Russian-Aligned Group Targets OT/ICS,* Forescout, 9 X 2025, https://www.forescout.com/blog/anatomy-of-a-hacktivist-attack-russian-aligned-group-targets-otics/ [accessed: 12 X 2025].

act on behalf of the Russian services. In January 2025, the Ukrainian Molfar Intelligence Institute published data on administrators and members of NoName057(16) and DDoSia groups carrying out DDoS attacks against websites and online services in countries opposed to the policy of the Russian Federation[43]. Julia Vladimirovna Pankratova, who was identified there, and Denis Olegovich Dekgtyarenko were included on the list of individuals sanctioned by the United States for their role in attacks by the CARR hacker group on the US critical infrastructure[44]. Analysts at Mandiant, the US cybersecurity company, pointed out in their report on the Sandworm group (identified as the military unit 74455 within the Main Centre for Special Technologies of the GRU) its links to XakNet, Solntsepek and CARR collectives[45]. This most likely means that the CARR and the groups working in alliance with it carry out tasks on behalf of the Russian Federation, which calls into question the grassroots nature of hacktivism.

Supply chain security

One of the most important conclusions of the CSIRT GOV report is to draw attention to the growing risk associated with third parties – IT service providers, outsourcing companies and contractors. Supply chain incidents show that organisation's security is only as strong as the weakest link in its ecosystem. Restrictive internal procedures do not guarantee security if external partners do not maintain an adequate level of protection[46]. In 2024, incidents involving system compromises, data exfiltration and publication occurred in companies providing IT and automation services,

[43] *Russian Cyber Army. Who is it?*, Molfar Intelligence Institute, 23 I 2025, https://www.molfar.institute/en/russian-cyber-army/ [accessed: 12 X 2025].

[44] *Treasury Sanctions Leader and Primary Member of the Cyber Army of Russia Reborn,* U.S. Department of the Treasury, 19 VII 2024, https://home.treasury.gov/news/press-releases/jy2473 [accessed: 11 X 2025].

[45] G. Roncone, D. Black, J. Wolfram, T. McLellan, N. Simonian, R. Hall, A. Prokopenkov, D. Perez, L. Aytes, A. Wahlstrom, *APT44: Unearthing Sandworm,* https://*services*.google.com/fh/files/misc/apt44-unearthing-sandworm.pdf, pp. 12–13 [accessed: 19 III 2025].

[46] CSIRT GOV, *Report on the state of Poland's cybersecurity…*, p. 113.

e.g. AIUT Sp. z o.o.[47] and Atende S.A.[48] In 2025, these were EuroCert Sp. z o.o.[49], a provider of qualified signature services, and the security company Ekotrade Sp. z o.o.[50]. These actions resulted in the disclosure of sensitive data about employees, customers and contracts.

In the context of national security, this means that the supply chain must be treated as an integral part of the state's security system. Regular security audits, remote access control, data protection in transit and at rest, verification of contracts with suppliers, and the development of business continuity plans should be standard practice in public institutions and strategically important enterprises, including among critical infrastructure operators[51].

Summary

When analysing the CSIRT GOV report in a broader context, it should be noted that cyber attacks are increasingly becoming part of conflicts below the threshold of war, which fits in with Russia's concept of new-generation warfare. They serve to gather intelligence, spread disinformation and destabilise without the need to use military force. In this sense, cybersecurity is no longer just a technological domain, but also a strategic and political one, as it is an area where the interests of states, the private sector and society intersect. Attacks on public administration, critical infrastructure and public media have symbolic and psychological dimensions – they undermine trust in state institutions by exposing their weaknesses and generate media hype. The ability to respond quickly, inform

[47] *Incydent bezpieczeństwa* (Eng. Security incydent), Aiut, https://aiut.com/incydent-bezpieczenstwa/ [accessed: 12 X 2025].

[48] *Komunikat Atende w związku z upublicznieniem ukradzionych danych* (Eng. Atende statement regarding the disclosure of stolen data), Atende, 22 X 2024, https://atende.pl/pl/aktualnosci/komunikat-atende-w-zwiazku-z-upublicznieniem-ukradzionych-danych [accessed: 12 X 2025].

[49] *Atak na EuroCert – oświadczenie* (Eng. The attack on EuroCert – statement), EuroCert, 15 I 2025, https://eurocert.pl/atak-na-eurocert-oswiadczenie/ [accessed: 12 X 2025].

[50] *Komunikat dotyczący ataku hakerskiego na infrastrukturę informatyczną Ekotrade Sp. z o.o.* (Eng. Statement regarding the cyber attack on the IT infrastructure of Ekotrade Sp. z o.o.), https://ekotrade.com.pl/img/rodo/KOMUNIKAT-EKOTRADE-dla-pracownikow.pdf [accessed: 12 X 2025].

[51] CSIRT GOV, *Report on the state of Poland's cybersecurity…*, p. 116.

public opinion in accordance with established strategic communication scenarios, and restore organisation continuity is one of the most important aspects of defence.

The CSIRT GOV report confirms that the cybersecurity of the Republic of Poland is now an integral part of national security, and its maintaining requires synergy between the technical, legal and organisational activities of the state. The scale of threats to Poland is not diminishing, which is why it is so important that the ability of institutions to identify them, mitigate their effects and build resilience continues to grow. Cooperation and information exchange are very important. The constantly evolving national cybersecurity system, expanded to include sectoral CSIRT teams, together with national teams, competent cybersecurity authorities, operators of essential services and other institutions, must constitute an effective shield against threats of international nature. Security is a continuous process that requires constant verification, audits and flexibility in order to adapt to changing technological and geopolitical conditions. New vulnerabilities and attack techniques emerging every day, and above all, the development of artificial intelligence, which will support attackers in creating phishing content and new versions of malware, mean that it is necessary to increase one's resilience and ability to respond to emerging threats. This is more important than ever before.

The dynamically changing nature of threats in cyberspace highlights the urgent need to abandon the reactive model in favour of actions aimed at building Poland's cyberspace resilience. They should consist primarily of implementing comprehensive, system-level solutions, as well as improving internal organisational regulations. This direction is reflected in the proposed legislative changes, particularly in the amendment to the Act on national cybersecurity system and the Act on crisis management. Their implementation in 2025 aims to improve coordination of actions and exchange of information, take into account the vulnerability of supply chains, and increase the overall institutional resilience of the state to incidents in the cyberspace. The effectiveness of these solutions will largely depend on the extent to which they are implemented and on the ability to adapt in the face of further evolution of cyber threats.

Monika Stodolnik

Officer of the Internal Security Agency.

Contact: monika.stodolnik@abw.gov.pl