PRZEGLĄD ZACHODNI
2024, nr 4
doi.org/10.60972/PZ.2024.4.55

DOMINIKA LISZKOWSKA
Koszalin
ORCID: 0000-0001-6312-341X

Cybersecurity and Threats to Electoral Processes in Central European States on the Example of Poland and Germany

Introduction

According to the national security paradigm, the traditional role of the state is important in securing borders and enforcing the rule of law. In this context, security treated in a traditional (national) way is based on the issue of protecting the homeland (Tumkevič 2016: 74). In the traditional approach to security, the state is the main object of reference and a key actor in the implementation of security policy. Therefore, it is the state that holds power within its territory and has the right to exercise it to ensure security against external threats.

As some researchers suggest, the emergence of the Internet and the need to ensure cybersecurity have changed the role of state entities as key security actors. This is the result of the multi-aspect and comprehensive nature of cybersecurity policy, which requires the diversification of entities involved in its implementation (Kaklauskaitė 2020: 45). Therefore, cooperation with other internal entities (e.g. with the public sector in the field of raising public awareness), international experts, countries (such as the USA) and international organizations (European Union) (Bendiek, Schulze 2021) has become a prerequisite to ensuring cybersecurity (Kaklauskaitė 2020: 45). Progressing digitalization has expanded the sphere of threats in cyberspace, covering every aspect of the functioning of the state – from social life, through the economy, to the political sphere. New technologies, the progressive development of cyberspace, as well as the intensification of information warfare and the growing dependence on IT infrastructure have created a situation in which non-military defence has become almost as important as military defence (Kamiński, Śliwa 2023: 135), and cybersecurity has become of fundamental

importance both for military security and for other spheres functioning of the state.

In recent years many states, including Germany and Poland, have recognized the scale of cyber threats and the risks they pose to national security, democracy and stability, as well as public order and critical sectors of the economy. The change in the perception of dangers occurring in cyberspace is visible in national documents on this issue. For example, the German cyber strategy of 2011 included cyber threats much more generally than the document from 2016. The 2016 strategy included, among others: the consequences of threats to democracy or public order, recognizing a wide range of potential attackers and their motives (Wechsler 2020: 67), which was not specified in the 2011 document.

There is no doubt that cyberattacks carried out by authoritarian governments and non-state actors are a growing threat to democracy around the world. The emergence of non-traditional voting options (including e-voting) revealed a number of challenges and potential problems related to the integrity of the elections of the most important state authorities. They do not only concern the creators of the system and its operator, but may also have potential political consequences and issues related to the legitimization of the government, making it possible to undermine the election results (Gliwa 2019: 2). According to data from the Government of Canada (2023), cyber threat activity targeting elections has increased around the world. Between 2015 and 2022, the percentage of elections affected by cyber threats in relation to the total number of national elections in the world increased from 10% to 26%. Of the countries where national elections were the target of cyber threats, approximately 25% concerned NATO members and approximately 35% of OECD countries (Communications Security Establishment 2023). It should be noted that between July 2021 and June 2022, throughout the European Union, the largest number of incidents in cyberspace concerned the sphere of public and government administration (24.21%) (European Union Agency for Cybersecurity 2022), which is also important for ensuring the security of elections in the Member States.

In 2016, Germany was the EU state most frequently attacked by hackers (19%), both in the spheres of government, finance, production and telecommunications (FireEye 2017: 7). In turn, Poland, as a country directly neighbouring the territory of Ukraine, has become one of the main targets of cyberattacks related to the war that broke out in February 2022. According to Microsoft estimates, in 2024 Poland took fourth place in Europe among the most frequently attacked countries, after Ukraine, Great Britain and France (Duszczyk 2024).

The aim of this article is to present the issue of cybersecurity and threats to electoral processes in Poland and Germany, in relation to the last elections that took place in these countries. In the case of Germany, the analysis covers the period before the 2017 (2016) parliamentary elections until the next elections in 2021. In the case of Poland, however, the attention was focused on the last parliamentary elections in 2023. The research process is intended to answer the following question: what impact does the development of new electoral technologies, the problem of disinformation and foreign interference have on the security of electoral processes in the countries selected for analysis? To answer the above question, numerous documents were analysed, including reports of institutions and organizations such as: Federal Office for Information Security – *BSI* (Germany), *NASK* (Poland), NIS Cooperation Group and Commonwealth Secretariat.

Security of Voting Systems and Electoral Processes

Marcin Gogolewski and Michał Ren distinguish three types of voting systems in terms of the security model, without the use of a traditional voting card. These are systems with voting at polling stations, voting systems using public terminals and online voting (Gogolewski, Ren 2014: 313). In systems with voting at polling stations, the voter appears in person in order to vote using a machine. Activities such as confirmation of identity or voter authorization can be performed on-site by authorized officials. By definition, in this system, machines and polling stations constitute a controlled environment of the electoral process.

In the case of voting systems using public terminals, publicly available machines, such as ATMs or other dedicated computers, are used. Unlike the entire voting environment, only machines are subject to control. It is not possible, for example, for trustees to perform their functions. Online voting, on the other hand, takes place in an environment that is not subject to control. The voter casts a vote using personal equipment, at home. Only the voting system infrastructure, consisting of servers and their software, can be controlled by a trusted third party. This type of system is the most demanding in terms of security. Therefore, in practice, special mechanisms are used, such as voting cards (containing encoded information) or chip cards, which are characterized by relative trust (Gogolewski, Ren 2014: 313-314).

However, in the electoral space, digital technology is used to support numerous activities. These include: political campaigns, communication with

voters *via* social media, voter registration, casting or sending ballots, counting votes and, finally, disseminating the results (NASS 2023: 2). By exploiting technical vulnerabilities or by creating the impression that such vulnerabilities exist, cyber threats can undermine electoral integrity (Van der Staak, Wolf 2019: 15). The issue becomes even more complicated when people participating in the electoral system are taken into account. Parties and their staffs conducting political campaigns on the Internet make significant use of social media and user data. This is done to reach voters through direct marketing, targeted advertising, as well as communication tools for internal planning and organization (Commonwealth Secretariat 2020: 25).

Sam Van der Staak and Peter Wolf divide cyber threats to electoral processes into two categories: 1) attacks targeting election-related technologies, and 2) disinformation campaigns targeting the perceived integrity of the electoral process (Van der Staak, Wolf 2019: 15). Unlike campaigns that aim to influence voters, attacks on electoral infrastructure are intended to directly modify the election result or limit access to voting. Such attacks may take place at three stages of the electoral process, violating its integrity, i.e. (1) during the voter registration period, (2) during the voting itself, (3) when the votes are counted (Communications Security Establishment 2023). Taking into account the number of digital attacks on electoral infrastructure (in 2015-2022), although it began to increase slightly (Commonwealth Secretariat 2020: 25) in the period 2018-2020, its decline was visible in the following years. This trend is slightly different for influence attacks, political party cybersecurity and disinformation attacks. Their number in 2022 has increased significantly (Communications Security Establishment 2023).

Attackers targeting electoral processes can be defined as entities (individuals or groups) seeking to harm a given country by disrupting its activities, gaining access to information, and using it for destructive purposes. (National Democratic Institute). Entities threatening electoral processes in cyberspace are primarily nation states or entities sponsored by nation states, black-hat hackers, criminals, terrorists, and people using confidential information (insiders). Hacktivists and politically motivated groups are also mentioned as a potential source of attacks (The EU Cybersecurity Agency 2019: 5). Attackers may therefore pose different threats and have different resources and capabilities (National Democratic Institute).

One of the disruptions to the fair course of elections when using means in cyberspace is the motivation of actors. Interference in the electoral process may result from an attempt to undermine trust in democracy or overthrow the political opposition, the desire to cause chaos, anarchy and social divisions,

delegitimization as well as the shape of the foreign policy and national interests of other countries (attackers) attempting to gain potential geopolitical influence (The EU Cybersecurity Agency 2019: 5).

The goals of threat actors can be divided into three categories: short-term goals, medium-term goals, long-term goals (Communications Security Establishment 2023). Short-term goals include: (1) undermining the election results, (2) promoting polarization political discourse, (3) manipulating social media algorithms using fake bot accounts, (4) reducing voter turnout, (5) generating misleading videos, deepfakes, as well as other synthetic content generated by artificial intelligence. The medium-term goals relate to: (1) weakening trust in leadership, (2) one-sided public discourse on the Internet, whereby political polarization fuels discontent and social movements, (3) weakening trust in electoral infrastructure, (4) increasing scepticism about available information online. Finally, the long-term goals of cyberspace attacks include: (1) distrust in the democratic nature of the electoral process, (2) organizing domestic social movements to promote foreign economic, military or ideological interests, (3) giving up voting rights and apathy towards elections, (4) lack of trust in the content available on the Internet (Communications Security Establishment 2023).

Cybersecurity of Electoral Processes in Germany in 2016-2021

According to the general report of the Science and Technology Committee of the NATO Parliamentary Assembly, Germany several times found itself in a situation of threats to its electoral processes, which may have been related to the Russian Federation (Davis 2018: 8). In recent years, discrediting the electoral process in democratic countries as an expression of the will of citizens of other states has become part of the logic of Russia's hybrid war. In turn, systematic interference in foreign electoral processes turned out to be a real tool for achieving Moscow's own geopolitical goals (Kruglashov, Shvydiuk 2020: 82).

In Germany, voters still cast their votes in elections *via* paper ballots. However, a wide range of information technologies are used in the electoral process and voting environment, including: for internal and external communication of information, both public and non-public. However, the electoral process is subject to constant digitalization, and this has been particularly deepened by the Covid-19 pandemic (Bednarski 2023: 27). Which is why, even more activities of candidates and political parties were moved online.

Attacks targeting the electoral process, the voting environment and the information provided to voters may threaten the availability, confidentiality, in-

tegrity and authenticity of information technology (Federal Office for Information Security 2021: 74). Cybersecurity is exposed to a fully personalized spear phishing attack preceded by environmental intelligence. Unlike phishing, in this form of attack, victims are selected according to individual criteria (Kulik 2013) and then an infected e-mail is sent to them. In May 2016 Trend Micro, a company specializing in the production of security software, announced that the party of German Chancellor Angela Merkel had become a victim of this type of attacks. As a result of spear phishing, members of the Christian Democratic Union (*CDU*) received e-mails leading to a copied login screen for the webmail service they were using. In this way, the attackers were able to obtain login details (NIS Cooperation Group 2018: 9).

Cybersecurity experts blamed the incident on hackers APT28/Pawn Storm, an organization considered one of the longest-running cyber espionage groups that targets critics of the Russian government (Auchard 2016). According to Arne Schönbohm, then president of the Federal Office for Information Security (*BSI*), the group's first attack took place in May 2016. At that time, the attackers tried to create a *CDU* Internet domain in the Baltic region. The second attack was observed in August 2016. It was the aforementioned spear-phishing campaign carried out against German parties in the lower house of parliament. It was determined that the NATO domain name was used as part of the attack to introduce malware into the politicians' networks (Paganini 2016). The coordinated attacks involved credential phishing using computer services located in Latvia and the Netherlands (Auchard 2016).

Manipulation of public emotions can be considered one of the most effective measures taken as part of operations aimed at the electoral process. Disinformation, in which attackers attempt to undermine the credibility of elections, can occur at both international and domestic levels. These types of activities are an important tool for influencing society, including: by misleading about important issues raised during election campaigns (Van der Staak, Wolf 2019: 19-20) and may also be aimed at discrediting the entities responsible for conducting the elections, thus discrediting the election results. During the 2017 election period in Germany, one of the attempted manipulations was false information regarding the closing of polling stations at 15:00. Electoral officials were forced to explain *via* available instant messengers (Twitter) that this was false information and the polling stations would be open as before, i.e. until 6:00 p.m (Lüber 2021).

In order to carry out tasks related to the defence of the elections scheduled for September 24, 2017, the German authorities had previously distinguished two potential types of attacks: attacks targeting the electoral process and attacks

targeting directly or indirectly election campaigns (Brattberg, Maurer 2018). Numerous actions have been taken to minimize potential external influences. One of them were warnings addressed to Russia by the highest representatives of the German authorities, including President Frank-Walter Steinmeier. In March 2017, Chancellor Angela Merkel established the Federal Security Council of Germany. This body only meets when the country faces the most serious threats. One of the items on the agenda was protection against potential Russian interference in the September elections (Brattberg, Maurer 2018). In addition, the political parties concluded an agreement that, among other things, that they will not use information disclosed by cybercriminals for political purposes or use bots on social media. In cooperation with Google and Jigsaw, the "Protect your elections" package was developed, addressed to organizations participating in electoral processes in Germany and other countries. Another activity was also the creation of fact-checking teams and fact-checkers by media organizations that helped assess the authenticity of materials (Brattberg, Maurer 2018).

To counter disinformation attacks, the Federal Returning Officer and subordinate officials transmitted election information through various channels during the election period. It was the website, social media, press releases and interviews. Information was provided on Twitter and Instagram *via* the @Wahlleiter_Bund account, as well as on the website www.bundeswahlleiter.de, where a special section "Facts against fake news" was created (Lüber 2021).

The report "The State of IT Security in Germany in 2021", prepared by the Federal Office for Information Security, includes a special subchapter entitled "Cyber security for *Bundestag* and State Parliament Elections" (Federal Office for Information Security 2021). It presented, among others: activities that are applicable to securing the electoral process and environment. In order to protect the formal voting procedure and provide it with IT support, close cooperation is undertaken between *BSI* and the Federal Returning Officer, as well as the authorities of the individual states. To provide a comprehensive set of information and recommendations, including introducing further improvements to existing security measures, promoting the network as a source of up-to-date information and warnings, using the services of IT service providers, etc., many candidates and political parties use the *BSI* websites and services for customer groups (public administration and critical infrastructure).

BSI also provides support services to parties and candidates, such as securing their social media channels. This is due to the particular exposure of these people to cyberattacks due to their public position and activities. Enhanced monitoring measures apply during elections, including: public and social media. In addition, *BSI* participates in numerous working groups whose task is to

identify and assess threats, as well as take remedial actions. Reports, as well as warnings and notifications, are prepared for numerous stakeholders and then distributed *via* available communication channels (Federal Office for Information Security 2021: 74).

Despite numerous actions being taken, in September 2021, German media reported that the website of the body managing general elections in Germany was disrupted at the end of August. According to reports, the website where the official results were published was bombarded with data requests in a so-called distributed denial-of-service attack, causing servers to crash (AFP 2021). The event took place a week after the federal prosecutor's office announced that it had initiated an "investigation on suspicion of espionage" in connection with accusations made by German authorities that members of parliament were attacked with "phishing" attacks by Russian intelligence (The Straits Time 2021). During the key period of the election campaign, there were reports of cyberattacks aimed at taking over access passwords used by members of the *Bundestag* and the parliaments of the federal states. According to information provided by Andrea Sasse, spokeswoman for the German Ministry of Foreign Affairs, the authorities had reliable findings that the activities were attributed to the Ghostwriter hacking group, most likely linked to Russia and its *GRU* military intelligence service. The German government considered these actions unacceptable and a threat to Germany's security and democratic decision-making process, as well as a "serious burden on bilateral relations" (Liszkowska 2024: 87).

Cybersecurity of Electoral Processes in Poland (on the Example of the 2023 Parliamentary Elections)

Poland adopted a list of comprehensive changes to its cyberspace defence system. Cybersecurity has also become an integral part of state efforts towards national security and is often mentioned in other national strategic documents (Tumkevič 2016: 78-79). However, in the years 2015-2020 cyber threats that had a direct impact on Poland's internal security evolved. Of over one hundred thousand computer incidents in 2015-2019, as many as one third were cyber threats. In 2019 most of the malicious activities directed at Polish government administration networks came from Russian cyberspace (28%). Government institutions and critical infrastructure turned out to be the most affected (Kamiński, Śliwa 2023: 135-136). Poland's situation in cyberspace became even more serious after the outbreak of the war in Ukraine. In connection with the ongoing armed conflict, numerous cyber operations

have been observed, carried out both against Ukrainian entities and states supporting them. External threats focused on pre-access operations and intelligence gathering that would provide the armed forces with any tactical advantage. State-sponsored groups targeted 128 government organizations in 42 countries (European Union Agency for Cybersecurity 2022: 27). For strategic reasons, priority was given to, among others: countries bordering Russia and NATO members, including Poland.

Similarly to Germany, in Poland citizens must appear at a designated place or send a ballot by post to vote in the elections. However, the increasingly advanced digitalization of the electoral environment involves a high risk of cyberattacks at every stage of the process. A number of protection measures have therefore been taken ahead of the 2023 elections. One of them was the BezpieczneWybory.pl portal launched by *NASK*, with the support of Google, Meta and TikTok, constituting a compendium of electoral knowledge and voting security (jd 2023). It was addressed to all Internet users, including electoral committees, who could influence the implementation of protective measures in the field of cybersecurity incidents and disturbing content through the application form (*NASK* 2023: 2). According to the final report of *NASK*, in the period September 15 - October 15, 2023, 227 reports of election incidents were registered in Poland. During the election weekend (October 13-15, 2023), as many as 214 of them were registered (*NASK* 2023: 3). The most frequently repeated disinformation narratives concerned electoral fraud, manipulation of election results, intentional difficulties in voting for the Polish community and allowing Ukrainians to participate in the elections (*NASK* 2023: 3).

According to analyses by specialists from DFRLab, of the six abuses of electoral infrastructure articulated by the Atlantic Council (exploitation/use of infrastructure, vote manipulation, strategic publication, false involvement at the front, strengthening of sentiments and fabricated content) (Galante, Ee 2018), at least four of them were used before the elections out of 15 October 2023 in Poland by foreign entities (Fraser 2023). As reported, as part of the infrastructure exploitation, at least one phishing attack and numerous DDoS attacks were carried out by cybercriminals associated with Russian groups (Fraser 2023). In August 2023, the activities of the UNC1151 hacking group were detected in the Polish Internet. They involved impersonating two high-level Polish government officials and sending e-mails to politicians of the ruling Law and Justice party (*PiS*) (Gigitashvili 2023). The fake email attachment contained Cobalt Strike software, which, when installed, allows people to steal data, demand ransom or send malicious messages to subsequent recipients. After reporting the incident, CERT Polska contacted the e-mail service provider, which

helped limit the spread of the infected message (Bojanowicz 2023). A separate incident of infrastructure abuse concerned a series of DDoS attacks on Polish websites in August and September 2023. Details about the attack were published in early September 2023 on its Telegram by the NoName057(16) group. It was explicitly stated that they were related to the elections in Poland (Fraser 2023). The group disrupted access to many websites in the country, including: banking and financial institutions, the Supreme Court (Gigitashvili 2023) and most likely also the government service "trusted profile", which allows remote confirmation of identity and receipt of a digital signature (Duszczyk 2023). According to the authors of the Compendium on Elections Cybersecurity and Resilience, developed by the NIS Cooperation Group, Distributed Denial-of-Service (DDoS) attacks can be a very effective tool in undermining public trust in the electoral process. Their use in the most critical phases of elections, i.e. transmitting, aggregating and displaying voting results, poses a particular danger. It should be noted that attacks of this type took second place in the ETL 2023 ranking (21.4%) among all analysed cases that are important for election security (NIS Cooperation Group 2024: 5).

Although before the parliamentary elections (2023) in Poland, no strategic publication operations (public disclosure) of content illegally obtained *via* infrastructure took place. It was during the campaign that materials from hack-and-leak operations were used (Fraser 2023). It was about e-mails stolen from the e-mail address of the head of the Chancellery of the Prime Minister, Michał Dworczyk (*PiS*), which were published in 2021 on *Telegram*. They were used by the Civic Platform (*PO*) staff for the campaign before the 2023 elections. *PO* election videos published since August 21, 2023 are based on materials from Dworczyk's e-mail. They used, among others: the AI-generated voice of Prime Minister Mateusz Morawiecki (*PiS*), who read the content of e-mails from the hacked mailbox of the *PiS* minister (Jabłonowski, Kunert, Sieczkowska 2023) (initially, the publications did not contain information that artificial intelligence tools were used in them, this was confirmed on August 24, 2023). *PO* politicians did not agree with the opinion that it was a deepfake that should not be used in the campaign (Jabłonowski, Kunert, Sieczkowska 2023). However, according to Givi Gigitashvili, the party's actions can be considered controversial, because it was a foreign group of cybercriminals that carried out the initial hacking and content leaking operation. The phishing scam and hacking into the minister's mailboxes were probably carried out by a group of cyber spies whose goal was to destabilize the political situation in Central European countries (UNC115) (Michalik 2021). Thus, *PO* used this content to strengthen the activities of cybercriminals, providing additional visibility of the activities of

hostile foreign entities. Moreover, it should be noted that there is no knowledge about which content made available on the Internet by UNC115 was authentic and which was not. In this way, the staff could unknowingly lead to the reinforcement of lies created by a group of cybercriminals whose goal was to undermine the reputation of the attacked (Michalik 2021). Also, according to the NIS Cooperation Group, access to data collected as a result of this type of attack may mislead voters. Due to the exfiltration of internal party or government documents, disinformation campaigns are actually used. According to the ETL 2023 study, primarily phishing carried out *via* e-mail is one of the main vectors of initial infections and has a significant impact on the risk of using artificial intelligence in social engineering. You can use it to create more convincing e-mail content or deepfakes for voice cloning and data mining (NIS Cooperation Group 2024: 5).

Based on monitoring of the infosphere and reports of incidents received during the election period, a set of recommendations was prepared for state institutions, but also for society, also from the perspective of an individual network user. At the state level, they included: introducing appropriate legislation on the issue of disinformation (while maintaining a balance between limiting the impact of disinformation and respecting freedom of speech and press), cooperation with online platforms, educational campaigns, media education, supporting fact-checking and independent media, research and analyses, international cooperation, as well as transparency of state activities. According to *NASK* analysts, "it is important that the actions taken by the state to combat disinformation are transparent and properly justified. It's good for citizens to have confidence in the government's actions in this area" (*NASK* 2023: 21). In the case of society, it is important to report disinformation, support credible and independent media, and cooperate with the local community. In turn, every individual Internet user in Poland should consciously use social media, think critically and verify facts (*NASK* 2023: 21-23).

Conclusions

The electoral process currently depends on a wide range of different IT systems. Even though elections can be held traditionally, i.e. without the use of e-voting or devices supporting the voting process, they are still exposed to numerous attacks that may affect voters, trust in democracy and ultimately result. The phenomenon of globalization, the development of technology and the widespread use of the Internet have led to situations in which digital tools

are used at each stage of the electoral process. They are used to monitoring elections, count votes, announce results, and contact politicians with voters.

Cyberattacks on electoral processes, often carried out by foreign forces, may therefore have consequences even if they did not take place or were unsuccessful. Actions aimed at public institutions constitute the basis for authenticating forged documents, manipulating public opinion, and changing society's perception of issues important for elections. As the examples of Germany and Poland show, Central European countries are also exposed to threats in cyberspace, and this threat has even increased as a result of the outbreak of the war in Ukraine. Further activities to strengthen cybersecurity are therefore particularly significant, not only during the election of the most important authorities in the state, but also in the period between individual elections. Actions aimed at government institutions, political parties and individual candidates have consequences in a broader electoral perspective and may significantly change the result of the next elections in a given state.

Bibliography

AFP (2021), *German Election Authority Confirms Likely Cyber Attack*, https://www.securityweek.com/german-election-authority-confirms-likely-cyber-attack/ (access: 12.09.2024).

Auchard E. (2016), *Hackers try to attack Merkel's party, security consultants say*, https://www.reuters.com/article/idUSKCN0Y22KV/ (access: 12.09.2024).

Bednarski P. (2023), *Wpływ pandemii COVID-19 na cyfryzację administracji publicznej [online]*, Wrocław 2023, access: http://www.repozytorium.uni.wroc.pl/Content/140199/PDF/02_P_Bednarski_Wplyw_pandemii_Covid-19_na_cyfryzacje_administracji_publicznej.pdf (access: 12.09.2024).

Bendiek A., Schulze M. (2021), *The weak European reflex in the German Cyber Security Strategy 2021*, https://www.swp-berlin.org/en/publication/the-weak-european-reflex-in-the-german-cyber-security-strategy-2021 (access: 12.09.2024).

Bojanowicz R. (2023), *Atak pishingowy na skrzynki polityków i sympatyków PiS. Odpowiadają za to hakerzy powiązani z rosyjskimi GRU*, https://forsal.pl/lifestyle/technologie/artykuly/9283560,atak-pishingowy-na-skrzynki-politykow-i-sympatykow-pis-odpowiadaja-za.html (access: 12.09.2024).

Brattberg E., Maurer T. (2018), *Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks*, https://carnegieendowment.org/2018/05/23/russian-election-interference-europes-counter-to-fake-news-and-cyber-attacks-pub-76435 (access: 12.09.2024).

Commonwealth Secretariat (2020), *Cybersecurity for Elections: A Commonwealth Guide on Best Practice*, London.

Communications Security Establishment (2023), *Cyber threats to Canada's democratic process – 2023 update*, https://www.cyber.gc.ca/sites/default/files/cyber-threats-canada-democratic-process-2023-update-v1-e.pdf (access: 12.09.2024).

Davis S. (2018), *Russian Meddling in Elections and Referenda in the Alliance*, https://www.nato-pa.int/download-file?filename=/sites/default/files/2018-11/181%20STC%2018%20E%20fin%20-%20RUSSAN%20MEDDLING%20-%20DAVIS%20REPORT.pdf (access: 12.09.2024).

Duszczyk M. (2024), *Duży popyt na „cyberbezpieczników". Polska jest celem hakerów*, https://www.rp.pl/biznes/art39977141-duzy-popyt-na-cyberbezpiecznikow-polska-jest-celem-hakerow (access: 12.09.2024).

Duszczyk M. (2023), *Groźni rosyjscy hakerzy znów atakują Polskę. Celem GPW, banki, Profil Zaufany*, https://www.rp.pl/finanse/art39021181-grozni-rosyjscy-hakerzy-znow-atakuja-polske-celem-gpw-banki-profil-zaufany (access: 12.09.2024).

European Union Agency for Cybersecurity (2022), *ENISA Threat Landscape 2022*E, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022 (access: 12.09.2024).

Federal Office for Information Security (2021), *The State of IT Security in Germany in 2021*, Berlin.

FireEye (2017), *Cyberthreats: A perfect storm about to hit Europe*, https://www.marsh.com/content/dam/marsh/Documents/PDF/UK-en/cyber-threats-a-perfect-storm-to-hit-europe.pdf (access: 12.09.2024).

Fraser M. (2023), *Polska. Rosja i Białoruś próbowały wpłynąć na wybory*, https://cyberdefence24.pl/armia-i-sluzby/polska-rosja-i-bialorus-probowaly-wplynac-na-wybory (access: 12.09.2024).

Galante L., Ee S. (2018), *Defining Russian election interference: An analysis of select 2014 to 2018 cyber enabled incidents*, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/defining-russian-election-interference-an-analysis-of-select-2014-to-2018-cyber-enabled-incidents-2/ (access: 12.09.2024).

Gigitashvili G. (2023), *How foreign actors targeted Polish information environment ahead of parliamentary elections*, https://dfrlab.org/2023/12/13/how-foreign-actors-targeted-polish-information-environment-ahead-of-parliamentary-elections/ (access: 12.09.2024).

Gliwa S. (2019), *E-wybory – bezpieczeństwo czy wygoda? [ANALIZA]*,https://cyberdefence24.pl/polityka-i-prawo/e-wybory-bezpieczenstwo-czy-wygoda-analizas (access: 12.09.2024).

Gogolewski M., Ren M. (2014), *Bezpieczeństwo wyborów elektronicznych*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego. Ekonomiczne Problemy Usług" nr 112: 311-319.

Jabłonowski K., Kunert J., Sieczkowska G. (2023), *PO w spocie o „mailach prawdy" użyła sztucznej inteligencji*, https://tvn24.pl/wybory-parlamentarne-2023/po-w-spocie-o-mailach-prawdy-uzyla-sztucznej-inteligencji-st7311972 (access: 12.09.2024).

jd (2023), *NASK uruchomił portal Bezpieczne Wybory*, https://www.wirtualnemedia.pl/artykul/nask-bezpieczne-wybory-google-meta-tiktok (access: 12.09.2024 r.).

Kaklauskaitė M. (2020), *Multi-level Governance in Cybersecurity: What Role for the European Regions?*, "European Cybersecurity Journal" vol. 6: 44-51.

Kamiński M. A., Śliwa Z. (2023), *Poland's Threat AssessmentDeepened, Not Changed*, „PRISM" vol. 10, nr 2: 131-147.

Kruglashov A., Shvydiuk S. (2020), *Hybrydowe zagrożenia dla demokracji. Wybrane przykłady zewnętrznej ingerencji Rosji w wybory*, „Wschód Europy" vol. 6, nr 2: 79-93.

Kulik W. (2013), *Co to jest spear phishing i czym grozi?*, https://www.benchmark.pl/aktualnosci/spear-phishing-co-to-jest-ataki-coraz-popularniesze.html (access: 12.09.2024 r.).

Liszkowska D. (2024), *Cyberataki na procesy wyborcze w Republice Federalnej Niemiec w latach 2015-2021*, w: Karpiuk A. (red.), *Cyberbezpieczeństwo. Aspekty krajowe i międzynarodowe*, Warszawa 2024.

Lüber K. (2021), „*Stable and secure". Is the election in Germany threatened by manipulation? The Federal Returning Officer explains the precautions that are being taken*, https://www.deutschland.de/en/topic/politics/election-in-germany-protection-against-manipulation (access: 12.09.2024.).

Michalik B. (2021). „*Rzeczpospolita": Hakerzy mieli dostęp do poczty ministra Dworczyka od 9 miesięcy*, https://www.komputerswiat.pl/aktualnosci/wydarzenia/afera-mailowa-pierwsze-wlamanie-na-konto-michala-dworczyka/mg6rlcp (access: 12.09.2024).

NASK (2023), *Bezpieczne wybory – raport zamknięcia*, https://www.bezpiecznewybory.pl/api/download-file?fileId=1919 (access: 12.09.2024 r.).

NASS (2023), *5 Elements of Cybersecurity for Election Offices*, https://www.nass.org/sites/default/files/2023-02/Smartmatic-White-Paper-NASS-Winter23.pdf (access: 12.09.2024).

National Democratic Institute (2022), *Cybersecurity Handbook for Political Parties A guide for political parties looking to get started on a cybersecurity plan – Introduction,* https://parties.cyberhandbook.org/introduction (access: 12.09.2024).

NIS Cooperation Group (2024), *Compendium on Elections Cybersecurity and Resilience*, https://digital-strategy.ec.europa.eu/en/news/new-cybersecurity-compendium-how-protect-integrity-elections-published (access: 12.09.2024).

NIS Cooperation Group (2018), *Compendium on Cyber Security of Election Technology*, https://ec.europa.eu/information_society/newsroom/image/document/2018-30/election_security_compendium_00BE09F9-D2BE-5D69-9E39C5A9C81C290F_53645.pdf (access: 12.09.2024).

Paganini P. (2017), *Top German official said Germany blocked Russian APT28 cyber attacks in 2016*, https://www.cyberdefensemagazine.com/top-german-official-said-germany-blocked-russian-apt28-cyber-attacks-in-2016/ (access: 12.09.2024).

The EU Cybersecurity Agency (2019), *Election cybersecurity: Challenges and opportunities*, https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/election-cybersecurity-challenges-and-opportunities (access: 12.09.2024.).

The Straits Time (2021), *German election authority confirms likely cyber attack*, https://www.straitstimes.com/world/europe/german-election-authority-confirms-likely-cyber-attack (access: 12.09.2024).

Tumkevič T. (2016), *Cybersecurity in Central Eastern Europe: from identifying risks to countering threats*, "Baltic Journal of Political Science" nr 5: 73-88.

Van der Staak S., Wolf P. (2019), *Cybersecurity in Elections Models of Interagency Collaboration*, Stockholm.

Wechsler O. (2020), *Back to the Civilian Power Discourse: Can it Survive in Cyberspace?*, "European Cybersecurity Journal" vol. 6.

Dr Dominika Liszkowska, Katedra Studiów Regionalnych i Europejskich, Wydział Humanistyczny, Politechnika Koszalińska (dominika_liszkowska@wp.pl)

Słowa kluczowe: wybory, cyberbezpieczeństwo, Polska, Niemcy, procesy wyborcze

Keywords: elections, cybersecurity, Poland, Germany, electoral processes

ABSTRACT

Many states, including Germany and Poland, have realized in recent years how serious cyberthreats are and what dangers they pose to national security, democracy and stability. National documents on the subject demonstrate the shift in the way that threats in cyberspace are perceived. Cyberattacks by non-state actors or authoritarian governments are unquestionably becoming a graver threat to democracy and state security. As a result of the introduction of non-traditional voting methods, such as e-voting, and the extensive digitization of the electoral process, a number of challenges and potential problems related to the integrity of elections have surfaced at every level.

The aim of the article is to present the cybersecurity concerns and threats to Germany's and Poland's electoral processes related to the recent national elections in these countries. The goal of the research is to determine how the security of election processes in particular states is affected by the emergence of new electoral technologies, the issue of disinformation, and foreign interference.