mgr inż. Dawid Kądzioła
University of Agriculture, Faculty of Production and Power Engineering,
Department of Machinery Operation, Ergonomics and Production Processes
e-mail: dawid.kadziola@icloud.com
ORCID: 0009-0006-4464-4803

DOI: 10.26410/SF_2/25/7

CYBERSECURITY AS A KEY ELEMENT OF NATIONAL SECURITY: AN ANALYSIS OF THREATS AND DEFENSE STRATEGIES IN THE 21st CENTURY

Abstract

The aim of this article is to analyze the key role of cybersecurity in ensuring national security in the 21st century. First, the theoretical foundations of cybersecurity and the current legal framework are presented, with particular emphasis on the Polish national cybersecurity system and EU regulations, such as the NIS and NIS 2 directives. Next, the main cyber threats to the state are identified and discussed, including attacks on critical infrastructure, ransomware threats, disinformation activities, and organizational gaps and human error. The article provides a detailed analysis of cyber threat defense strategies, emphasizing the importance of synergy between the public and private sectors and the services responsible for security. The methodology used includes an analysis of scientific literature, legal acts, strategic documents, and reports from CERT/CSIRT teams. The conclusions of the analysis point to the need for a holistic approach to cybersecurity, integrating political, legal, technical, and educational measures, which is a prerequisite for effectively countering growing cyber threats.

Keywords

cybersecurity, national security, critical infrastructure, cyber threats, defense strategies

Introduction

In the era of widespread digitization, cybersecurity has become an integral part of national security. Critical state infrastructure, public services, and the private sector increasingly rely on ICT systems, which brings with it new types of threats. The scale of these threats is growing rapidly–for example, according to FBI data, 2020 saw a 400% increase in the number of cyberattacks[1] – and similar trends are observed in Poland, where CERT Polska recorded as many as 34% more cybersecurity incidents than in the previous year. Cyberattacks are no longer isolated incidents – they are now a daily challenge for public administration at all levels. The consequences of successful cyberattacks can be very serious. Disruption of the power grid, financial system, or transportation system threatens the stability of the state in a way comparable to traditional physical threats. The disclosure or encryption of sensitive citizen data undermines trust in public institutions and compromises the privacy of society. Cyber-attacks can also limit the state's ability to provide basic services and respond to emergencies. Cybercrime poses a threat not only to the efficient functioning of local governments, but also to the entire state and the security of its citizens[2]. For this reason, countries around the world have recognized cyberspace as a key area of their security strategy.

This article analyzes the most serious cybersecurity threats to state security in the 21st century and presents defense strategies, with particular emphasis on the Polish legal and institutional context.

Theoretical part

Cybersecurity is sometimes defined in legal terms as "the resilience of information systems against actions that violate the confidentiality, integrity, availability, and authenticity of processed data or related services," as stated in the Act of July 5, 2018, on the national cybersecurity system[3]. This definition emphasizes that the essence of cybersecurity is to ensure the continuity and trustworthiness of information and communication systems despite attempts at disruption or attacks. Cybersecurity has become an integral part of national security, as modern states cannot function without efficient IT systems supporting administration, the financial sector, energy, communications, healthcare, and other key services. a breach of cybersecurity can therefore translate into real threats to public order, the economy, and even the lives of citizens.

In response to growing threats, Poland, like other European Union countries, has developed a legal and institutional framework to protect cyberspace. The aforementioned Act on the National Cybersecurity System of 2018 implements the provisions

1 A.F. Ruggiero, T. Owosu, *Ransomware in local government: Risk factors, vulnerabilities, and exploitation during a global pandemic*, Issues in Information Systems 2022, No 23(4), p. 184.

2 T.T.P. Cortese, J.F.S.d. Almeida, G.Q. Batista, J.E. Storopoli, A. Liu, T. Yigitcanlar, *Understanding Sustainable Energy in the Context of Smart Cities,* a Prisma Review Energies 2022, No 15, 2382, p. 3.

3 Act on the National Cybersecurity System of 5 July 2018. (2018). *Journal of Laws of the Republic of Poland*, item 1560, as amended.

of the EU's 2016 NIS Directive (Network and Information Systems), defining the organization of the cybersecurity system at the national level. In accordance with the Act, the National Cybersecurity System (KSC) was established to ensure the uninterrupted provision of IT services and efficient incident management[4]. The system includes, among others, operators of essential services (OUK) in designated sectors, digital service providers, computer incident response teams (CSIRT) at the national and sectoral levels, as well as administrative bodies responsible for cybersecurity. According to the Act, operators of essential services are entities from sectors as important as energy, transport, banking and financial market infrastructure, healthcare, drinking water supply and digital infrastructure[5]. The Act imposes a number of obligations on these entities and selected administrative bodies, including the implementation of adequate security measures, conducting risk analyses, and reporting incidents within 24 hours of their detection to the relevant CSIRTs. Importantly, every serious or critical incident must be handled in cooperation with the relevant authorities, ensuring the exchange of information and necessary data. Such a reporting and response system aims to quickly stop the spread of attacks and limit their impact. Within the KSC, there are three main national CSIRT teams – at the Internal Security Agency (CSIRT.GOV), the Ministry of National Defense (CSIRT.MON) and the Research and Academic Computer Network (CSIRT.NASK) – which coordinate incident response in their respective areas. In addition, there are sectoral cybersecurity teams, and the relevant ministers perform coordination functions in specific sectors (e.g., energy, transport, healthcare). The entire system is supported by a central coordinator, currently the Chancellery of the Prime Minister through the Secretariat of the Government Plenipotentiary for Cybersecurity. The Polish model is therefore sectorally dispersed but with central strategic coordination – the Cybersecurity Strategy of the Republic of Poland for 2019-2024 sets out the objectives and directions of state policy in this area (replacing the previous Cybersecurity Policy Framework 2017-2022). The NIS Directive has laid the foundations for a coherent and integrated cybersecurity system in Europe, strengthening protection against growing threats in cyberspace[6]. In 2022, the EU adopted the new NIS 2 Directive, which further expands the scope of entities covered by the regulations (including medium-sized enterprises from additional sectors, election administration, space, postal services, etc.) and tightens requirements for incident reporting and risk management. NIS 2 emphasizes, among other things, increasing the responsibility of management for cybersecurity in organizations and strengthening cross-border cooperation. The implementation of this directive into Polish law will further strengthen the system and adapt it to the evolving threat landscape.

4 M. Terlecka-Maciejewska, *Cybersecurity in Polish security system*. Zeszyty Naukowe Politechniki Śląskiej, seria Organizacja i Zarządzanie 2024, No 198, pp. 561–571.

5 A. Chodakowska, S. Kańduła & J. Przybylska, *Cybersecurity in the Local Government Sector in Poland: More Work Needs to be Done*. Lex Localis – Journal of Local Self-Government, No 20(1), pp. 161–192.

6 Ibidem pp. 161-192.

In addition to legal regulations, the theoretical dimension of cybersecurity is constituted by information security management norms and standards. International standards, such as ISO/IEC 27001 or the American NIST Cybersecurity Framework, provide systematic methods for risk assessment and implementation of appropriate security measures. Research has shown that a significant proportion of Polish local government units have implemented an Information Security Management System (ISMS) – in one study, as many as 76.9% of municipalities declared that they had such a system, of which 82.2% complied with the ISO 27001 standard[7]. Standardizing security practices and having a formal policy increases resilience to attacks, although, as the audit results show, simply having documents is not enough. Effective implementation of policies in practice and raising staff awareness are key. For this reason, cybersecurity theory emphasizes a holistic approach that combines technical, organizational, and human aspects. In particular, the concept of a socio-technical system highlights that security is not just about hardware and software, but also about people–their knowledge, habits, and adherence to procedures[8]. People are often the weakest link in a system, so factors such as safety culture and user education must be taken into account in the overall security strategy.

To sum up the theoretical part, a 21st-century state must view cybersecurity as an element of national security. Building resilience requires a legal framework, institutions responsible for response, the application of standards, and continuous awareness-raising and competence-building in the field of cyber threats. Only an integrated approach, involving cooperation between multiple actors and consistency of action, can address the nature of threats emanating from cyberspace.

Risk analysis

Contemporary cyber threats to national security are diverse and constantly changing. The most important categories include attacks on critical infrastructure, ransomware, disinformation, and organizational vulnerabilities (internal errors and negligence). These threats are discussed below, along with examples of their impact on national security.

Attacks on critical infrastructure

Critical infrastructure includes systems and facilities that are essential for the functioning of the state and society, such as energy networks, water supply, communication systems, transport, financial infrastructure, and healthcare. Cyber attacks targeting critical infrastructure can cause physical disruptions to the provision of essential services. For example, the high-profile attack on Ukraine's power grid in

7 Ibidem, pp. 161-192.

8 M. van Haastrecht, B. Yigit Ozkan, M. Brinkhuis & M. Spruit, *Respite for SMEs: a Systematic Review of Socio-Technical Cybersecurity Metrics*. Applied Sciences 2021, No 11(15).

December 2015 caused a temporary power outage for approximately 225,000 customers, demonstrating the potential of a cyberattack to cause a real energy crisis. This was the first documented case of a successful disruption of an electricity grid using malware (BlackEnergy). a year later, Ukraine again experienced a cyberattack (Industroyer) on its electrical infrastructure, confirming experts' belief that cyberattacks have become a tool not only for criminal groups, but also for hostile states and terrorists. Wide-ranging incidents have also been reported in other countries: in 2021, a ransomware attack on the Colonial Pipeline fuel pipeline in the US paralyzed gasoline distribution on the east coast, forcing a state of emergency to be declared for fuel supplies in the region. These examples prove that critical infrastructure is a target for cybercriminals and hostile states, and that a successful attack can disrupt a country as severely as traditional acts of sabotage. Poland has not yet experienced a cyberattack on critical infrastructure with effects comparable to the above examples, although attempts and incidents on a smaller scale have taken place. In 2020, the local government railways in the West Pomeranian Province were the victim of an attack that briefly disrupted train control systems–an incident that was also considered a potentially dangerous precedent in the transport sector. In August 2023, the media reported on the disruption of the PKP railway network due to unauthorized transmission of "radiostop" signals, which was identified as a possible hybrid operation with a cyber component. The energy and financial sectors are constantly being tested for resilience – APT (Advanced Persistent Threat) attacks, often attributed to foreign intelligence services, attempt, for example, to penetrate the networks of power plants or banks for the purpose of long-term, difficult-to-detect espionage or sabotage. Threats to critical infrastructure are therefore very real, and their materialization could threaten national security, public order, and even the health and lives of citizens on a massive scale. The literature on the subject emphasizes that the growing number of systematic attacks on critical infrastructure is a global problem and requires effective international cooperation and the development of standards for regulating cyberspace[9].

Ransomware – digital extortin

Ransomware is malicious software that encrypts a victim's data and demands a ransom for its decryption. In recent years, ransomware has grown into one of the most serious threats to public institutions and businesses. These attacks have evolved from randomly infecting home users to deliberate "big game hunting" – targeting critical or high-value organizations such as hospitals, government agencies, universities, and large enterprises[10]. Local governments have become a particularly frequent target of

9 T. Baranovska, V. Savitskyi, M. Serbov, Y. Stoliar & Y. Krutik, *The impact of cybercrime on state and institutional security: Analysis of threats and potential protection measures.* Economic Affairs 2024, No 69 (Special Issue), pp. 33–42.

10 A. F. Ruggiero, T. D. Owusu & J. J. Staley, *Ransomware in local government: Risk factors, vulnerabilities, and exploitation during a global pandemic.* Issues in Information Systems 2022, No 23(4), pp. 183–191.

ransomware attacks because they hold valuable data and perform key functions for the community, while often having limited IT resources and outdated infrastructure, which makes them vulnerable to this type of attack. The effects of a ransomware attack on a government agency or institution can be serious: loss of access to systems and data paralyzes the provision of public services, from issuing documents to administering social benefits. In addition, the leakage or lack of control over citizens' data violates information security and trust in the authorities. Unfortunately, many of the entities attacked, lacking backups or contingency plans, succumb to pressure and pay ransoms to cybercriminals, which only fuels further attacks. For example, in the US, there have been high-profile cases of cities such as Atlanta and Baltimore, where ransomware attacks paralyzed city government operations for days. Atlanta suffered losses estimated at over $17 million in 2018 as a result of the SamSam attack, and Baltimore refused to pay the ransom in 2019, but the cost of rebuilding its systems exceeded $18 million – in the meantime, residents were unable to finalize real estate transactions or pay municipal bills, among other things.

Polish institutions are also not immune to such incidents. Ransomware attacks on local governments in Poland have occurred in recent years, as exemplified by the incident at the Marshal's Office of the Mazowieckie Province in December 2022. Files were encrypted as a result of malicious software, which was officially classified as a serious cybersecurity incident[11]. Similarly, the District Employment Office in Bartoszyce fell victim to an attack by a ransomware group called RansomHub, resulting in a potential breach of the personal data of the office's clients. Statistics show how widespread this problem has become – according to a report by Sophos, as many as 69% of local government institutions experienced a ransomware attack in 2022, which illustrates the scale of the threat[12]. Global data is also alarming – there has been a sharp increase in the number of ransomware attacks over the past few years. In 2020 alone, the frequency of such incidents increased several times worldwide, and cybercriminals developed entire models for carrying out attacks by less technically advanced criminals. Ransomware is therefore a hybrid threat – on the one hand, it is a form of criminal activity aimed at financial gain, damaging the financial interests and continuity of institutions; on the other hand, mass attacks of this type (e.g. the WannaCry[13] campaign in 2017) can destabilize the infrastructure of many countries simultaneously. Such attacks on hospitals or transmission networks can even endanger human lives (e.g., by blocking access to life-saving systems). Countering these attacks has therefore become a priority for many governments, and ransomware is considered one of the most serious threats to national security in cyberspace.

11 https://mazovia.pl/pl/bip/komunikaty/incydent-cyberbezpieczenstwa, access 28.04.2025 r.

12 Sophos. (2023). *The State of Ransomware in State and Local Government 2023. Retrieved from Sophos News* (news.sophos.com). – access 27.04.2025 r.

13 R. Fordoński, *WannaCry ransomware cyberattack as violation of international law*, Uniwersytet Warmińsko-Mazurski, Studia Prawnoustrojowe 2019, No 44, p. 47.

Disinformation and information warfare

In addition to purely technical attacks on systems, disinformation–the deliberate dissemination of false or manipulated information in the digital space, particularly on social media and online portals–is a significant strategic cybersecurity threat. Disinformation is a tool of so-called information warfare, often used by foreign states or organized groups to weaken social cohesion and undermine citizens' trust in democratic institutions. Unlike malware attacks, the aim of information attacks is not to directly damage IT infrastructure, but to "hack" into the public consciousness – creating divisions, spreading panic or influencing political decisions through mass propaganda campaigns on the Internet. An example of the effects of disinformation is its influence on electoral processes. The widely reported interference in the 2016 US presidential election involved, among other things, organized activity on social media, the creation of fake news, and targeted disinformation campaigns designed to polarize the electorate and influence the outcome of the election. Attempts at such information influence have also been observed in Poland–for example, during the 2018 local government campaign, the existence of fake accounts spreading false political content was revealed online. Another area of information attacks was the COVID-19 pandemic, when conspiracy theories and false information about vaccines and restrictions appeared en masse, weakening the state's efforts to combat the health crisis. Currently, in the context of the ongoing Russian-Ukrainian war, the services are warning of an intensification of pro-Kremlin disinformation aimed, among others, at at NATO's eastern flank–narratives undermining the sense of supporting Ukraine, scaring people with a refugee crisis, or slandering allies are meant to cause social unrest and reduce the political cohesion of the state.

The threat of disinformation lies in the fact that it is difficult to detect and neutralize by technical means. Combating it requires constant monitoring of information, cooperation with the media and online platforms, and raising awareness among recipients. Disinformation often accompanies other forms of aggression–it can be part of broader hybrid campaigns combining, for example, hacking attacks (the theft of compromising data) with its subsequent disclosure and manipulation of the narrative (so-called hack-and-leak). Organized disinformation campaigns pose a serious risk to national security, as they can lead to social chaos, riots, and even undermine a country's information sovereignty. In response, NATO and EU countries are developing counter-disinformation strategies. For example, the European Union has set up a special unit to combat disinformation (the East StratCom Task Force) and launched a rapid response system for fake news as part of the EU's security strategy. In Poland, the problem of disinformation has been recognized, among others, in strategic documents on information security, which point to the need to strengthen social resilience to manipulation.

Organizational gaps and internal factors

Last but not least, internal organizational gaps are another category of threats. These are shortcomings, oversights, and mistakes on the part of people, procedures, and organizational structures that enable or facilitate cyberattacks. As mentioned, the "human factor" is sometimes referred to as the weakest link in security[14]. Even the best technical safeguards can prove insufficient if users make simple mistakes or the institution fails to follow basic security rules. Typical internal problems include low awareness of threats and lack of employee training, inadequate security procedures (e.g., no password policy or access management), and shortages of qualified personnel and funding for cyber protection. Reports indicate that human error and negligence may cause even more incidents than deliberate attacks by external hackers. For example, in its 2019 report on cybersecurity in municipalities, the Supreme Audit Office (NIK) in Poland found that over 80% of the irregularities identified concerned the improper management of system user permissions. The audit revealed, among other things, frequent cases of weak passwords, shared user accounts, and failure to revoke permissions for former employees, creating vulnerabilities that could be exploited by attackers. Other dangerous practices observed include the opening of suspicious email attachments by untrained employees and the use of unsecured USB drives–the consequences of such behavior can be as serious as those of complex technical attacks, as they lead to malware infections or data leaks. Staffing and financial shortages are another aspect of organizational vulnerabilities. Small institutions (e.g., small municipalities, small businesses) often do not have the budget for cybersecurity specialists or modern security measures[15]. They are forced to rely on outdated systems that are easier to penetrate, or on the work of a single IT specialist performing multiple roles (without the possibility of specialization). Research in Polish local governments has shown that the most frequently cited problem in ensuring security is precisely the limitation of financial resources, which hinders both the purchase of technical solutions and the hiring of experts. In addition, some entities still do not conduct regular risk analyses or security audits–for example, almost 25% of municipalities in the study by Chodakowska et al. (2022)[16] admitted that it does not conduct a formal risk analysis of the loss of confidentiality, integrity, and availability of information, often justifying this by a lack of need or resources. Organizational gaps are also evident in the incomplete implementation of existing regulations. Despite the KSC Act being in force, some entities have not appointed a cybersecurity contact person or do not report incidents–the study cited showed that 44% of agencies that experienced incidents did not report them to the relevant authorities. Some organizations may be reluctant to disclose breaches for fear of consequences or loss of

14 M. van Haastrecht, B. Yigit Ozkan, M. Brinkhuis & M. Spruit, *Respite for SMEs: a Systematic Review of Socio-Technical Cybersecurity Metrics.* Applied Sciences 2021, No 11(15), p. 1

15 A. F. Ruggiero, T. D. Owusu & J. J. Staley, *Ransomware in local government: Risk factors…*, op. cit., pp. 183–191.

16 A. Chodakowska, S. Kańduła & Przybylska, *Cybersecurity in…*, op. cit., pp. 161–192.

reputation, which distorts the overall picture of threats and hinders the response at the national level. To sum up the threat analysis: the country faces both sophisticated external attacks and internal weaknesses in its own structures. Attacks on critical infrastructure and ransomware can cause direct crises and losses, disinformation undermines the foundations of public trust, and organizational gaps increase vulnerability to all of the above threats. Awareness of these threats is the starting point for designing adequate defense strategies.

Defense strategies

An effective national cybersecurity defense strategy must be multi-layered and comprehensive. There is no single remedy–a combination of legal, organizational, technical, and educational measures is needed, as well as close cooperation between the public and private sectors and citizens. The key pillars of a cyber defense strategy in relation to the previously identified threats are presented below.

Legal and institutional framework

The basis for defense is appropriate law and institutional structures. In implementing the NIS Directive, Poland established a National Cybersecurity System with clearly defined roles and procedures. The KSC Act obliges critical infrastructure operators and other key entities to maintain minimum security standards and to report and respond to incidents quickly[17]. This ensures that there is a formal response path in case of an incident: detection, notification of CSIRT, remedial action, and notification of other potentially affected entities. CSIRT teams act as first responders in cyber security – they analyze reports, support victims of attacks in restoring system functionality, and publish warnings about new threats. It is important to continuously improve their technical capabilities (e.g., investments in attack detection systems, development of threat intelligence) and ensure the rapid flow of information with private and foreign entities.

Another element is the state strategy – a strategic document setting out objectives and actions for the next few years. The current Cybersecurity Strategy of the Republic of Poland 2019–2024 emphasizes, among other things, the development of national incident response capabilities, the protection of critical infrastructure, the building of public awareness and competence, and international cooperation. The implementation of the strategy is coordinated by the Government Plenipotentiary for Cybersecurity, and progress is monitored. This type of document ensures an integrated approach, e.g., it links military issues (cyber defense in the Armed Forces) with civil issues (protection of administration networks) and the economy (increasing the resilience of infrastructure companies). Another important institutional

17 T. Baranovska, V. Savitskyi, M. Serbov, Y. Stoliar & Krutik, *The impact of cybercrime…*, op. cit., pp. 33–42.

initiative in Poland was the creation in 2022 of a Cyber Defense Forces component within the Armed Forces. These units (subordinate to the Cyber Defense Forces Component Command) are responsible for defensive and offensive actions in cyberspace for the purposes of national defense. Their existence strengthens the potential to respond to serious attacks (especially those sponsored by foreign countries) and enables active counteraction to threats within the framework of military operations. The combination of civilian (CERT/CSIRT) and military expertise in cybersecurity increases the state's ability to deter aggressors – it signals that Poland is not only capable of defending itself, but also of identifying the perpetrators of attacks and responding to them, including through legal measures or potential counterattacks (within the framework of international law).

Technical protection and best practices

At the operational level, it is crucial to implement specific technical measures and procedures that will make it difficult for attackers to achieve their goals. This is where the aforementioned standards and best practices come in handy. Every institution should implement multi-layered protection (*defense in depth*) – starting with network security (firewalls, intrusion detection systems), through workstation and server protection (up-to-date antivirus/EDR software, regular vulnerability patching), to data backup mechanisms and business continuity procedures (disaster recovery). In recent years, particular emphasis has been placed on access and identity management – for example, the implementation of two-factor authentication (2FA) for access to critical systems makes it significantly more difficult for attackers to take control even if passwords are leaked. Equally important is network segmentation (so that, for example, the infection of one computer does not immediately give access to the entire office network) and strict control of permissions (granting users only the minimum access necessary in accordance with the *least privilege* principle). Compliance with such rules could prevent many incidents reported by the NIK – for example, rigorous account management would eliminate the problem of universal passwords or active accounts of former employees.

In the context of ransomware, a technical defense strategy must include regular backups of critical data and systems and their secure storage (e.g., offline). This ensures that even if data is encrypted, the institution can restore its operations without paying a ransom. Many organizations that have fallen victim to ransomware have managed to recover thanks to backups. In addition, systems that detect unusual behavior indicative of a ransomware attack (e.g., mass file encryption operations) and automatically block such processes are becoming increasingly common. It is also essential to test your own security measures through audits and penetration tests. This allows you to identify vulnerabilities before a potential attacker does. For small entities that do not have their own experts, cooperation with external security auditors is a good solution – it is suggested, for example, that local governments could

use the services of specialists or certified providers (or even transfer some services to a cloud managed by trusted operators) to increase their level of data protection. This approach, while raising questions about trust in external partners, can be cost-effective and organizationally efficient for entities with limited resources. a large cloud provider is able to provide a level of security that is difficult to achieve locally. In summary, technical defenses must keep pace with threats: regular updates, patching vulnerabilities, monitoring systems, and contingency planning (backup, recovery) are the foundation of cybersecurity for any institution. Government policy should support the implementation of best practices, e.g. through the issuance of sectoral security guidelines, product certification (activities in this area are carried out, among others, by the EU Agency for Cybersecurity ENISA) or funding programs to increase security in critical sectors.

Cooperation between sectors

Cooperation between the public, private and civil sectors is absolutely crucial in the context of national cybersecurity. This is because a significant part of critical infrastructure and services (such as energy, telecommunications, banking) is owned or operated by private entities. The state is not able to secure the entire national cyberspace on its own–partnerships with businesses and the active involvement of citizens are needed.

At the national level, an example of cooperation is the creation of the Polish Cybersecurity Forum, a platform for the exchange of information between the administration, critical infrastructure operators, and experts. In addition, under the KSC Act, each key service operator is required to designate persons to liaise with the relevant authorities and CSIRTs, creating a network for cooperation and communication in the event of an incident. At the EU level, there is the NIS Cooperation Group, where representatives of member states and CERT teams exchange knowledge about threats and best practices. The NIS and NIS 2 Directives formalize this EU cooperation as one of the pillars of common digital security.

In the public sector, the concept of public-private partnerships (PPPs) in the field of cybersecurity is increasingly being promoted. This involves, for example, government agencies cooperating with technology companies to share information on threats (known as *cyber threat intelligence sharing*), organize joint simulation exercises, or even set up sector-specific information sharing and analysis centers (ISACs). This enables companies to respond more quickly to warnings issued by the authorities, while the state gains insight into the situation beyond its own systems. This type of cooperation is facilitated by the establishment of voluntary incident reporting mechanisms by the private sector – in Poland, digital service providers (e.g., large internet platforms) are also subject to reporting obligations for serious incidents, which brings them closer to public sector standards. At the local level, it is worth creating partnerships between local governments – for

example, neighboring municipalities can share knowledge, jointly hire a security specialist, or co-finance security systems. Such solutions allow for economies of scale – a single small municipality may not have the resources for a full-time cyber team, but several together can. Horizontal cooperation can also involve the exchange of good practices and experiences from incidents so that other entities can learn from each other's mistakes. The third segment is society – citizens who are both potential victims of cyberattacks (e.g., phishing) and the first line of defense (through their conscious behavior). Raising public awareness of cybersecurity is a strategic defense measure. Educational campaigns on phishing recognition, strong passwords, online privacy, and critical thinking about information (fact-checking, fake news recognition) can significantly reduce the effectiveness of hostile actors. As experts point out, education is key to exposing weaknesses and promoting good practices in cybersecurity[18]. The state should invest in training programs–both for its own officials (e.g., mandatory cyber hygiene training in the administration) and for citizens (e.g., through the education system–elements of digital and media education in schools). a society that is more resistant to manipulation and cautious online is an important protective layer against social engineering attacks and disinformation campaigns. Of course, it should be remembered that too much centralization or excessive state interference can also be undesirable – autonomous action by local and private entities is valuable. Cybersecurity is a public good that is best protected through joint efforts. The state can act as a coordinator and catalyst: conducting audits, identifying gaps (but not necessarily punishing immediately – it is more important to fix weaknesses), and sharing resources (e.g., offering smaller entities technical support or access to state security platforms).

Incident preparedness and resilience

Even the best prevention cannot eliminate the risk of an incident 100%, which is why preparation for attacks and ensuring resilience are key elements of the strategy. This means that institutions must have business continuity plans (BCP) and incident response plans (IRP) in place. Regular simulation exercises (*drills*) – e.g., backup system restoration tests, malware detection response scenarios, or *table-top* exercises for management – allow you to check whether your staff knows what to do and what decisions to make in a crisis situation. At the national level, large-scale cybersecurity exercises are organized (in Poland, these include Cyberyoyo, Cyber-Poligon, etc.), which involve various services and the private sector in joint training to respond to complex attacks. This allows weak points in coordination and communication to be identified before a real incident occurs.

18 T.T.P. Cortese, J.F.S.d. Almeida, G.Q. Batista, J.E. Storopoli, A. Liu, T. Yigitcanlar, *Understanding Sustainable Energy…*, op. cit., pp. 3.

Resilience also means the ability to quickly restore key functions after an attack. In practice, if, for example, a hospital is attacked by ransomware, it should have procedures in place to switch to manual mode or alternative systems to ensure continuity of patient care. Public administrations should ensure that they have the ability to switch services in an emergency, for example by having backup servers (even offline) on which basic e-services can be run if the main data centers are down. Diversification and redundancy are classic security approaches that are also used in IT – you should not keep all your resources in one place or allow single points of failure to exist.

International cooperation in responding to cross-border incidents is also extremely important. Cyberattacks rarely stop at a single country's border – malware spreads globally, and botnets attacking services in Poland can be controlled from abroad. That is why Poland actively participates in NATO and EU cyber defense initiatives. NATO has, among other things, the Cyber Defense Center of Excellence (CCDCOE) in Estonia, known for its Locked Shields exercises, in which Polish specialists also participate, learning from international partners. In the event of a serious attack, Poland can count on allied solidarity mechanisms (Article 5 of the North Atlantic Treaty potentially also covers cyber attacks if their effects are serious) and on the assistance of specialized units, such as NATO Cyber Rapid Reaction Teams. This international cooperation is part of the defense strategy–it also acts as a deterrent (the aggressor knows that an attack on one country may be met with a response from many).

Recommendations

An analysis of threats and current strategies allows us to formulate a number of recommendations to strengthen cybersecurity as an element of national security. The most important recommendations are presented below:

- Integrated strategic approach: a holistic cybersecurity strategy combining civil and military, national and international aspects should be continued and developed. The new strategy (post-2024) should take into account the experience of recent years and the implementation of the NIS 2 Directive, ensuring consistency between the actions of all actors involved.
- Strengthening the legal framework: It is recommended that the NIS 2 Directive be swiftly transposed into national law and that the Act on Cybersecurity be amended to cover a larger number of sectors and entities relevant to security (e.g., county-level local government, the chemical sector, and the space industry). The law should also provide for mechanisms for effective enforcement of obligations (audits, incident reporting) without excessive administrative burden.
- Increased funding and resources: The government should provide additional funding for cybersecurity in the public sector, especially for local government units and small government agencies, which are currently facing financial

difficulties in meeting all requirements[19]. This could take the form of dedicated funds, grants, or EU operational programs supporting investments in digital security (e.g., system upgrades, training, hiring experts). These investments should be treated similarly to national defense spending.

- Staff development and education: It is necessary to intensify programs for training cybersecurity specialists, both at the higher education level (more courses and places in IT studies with a specialization in security) and through certified professional training. For public administration, it is worth implementing a system for confirming competences (e.g., mandatory cybersecurity certificates for system administrators in government offices). In addition, public education on the basics of cyber hygiene and countering disinformation should become part of the state's information policy (public campaigns, school programs, cooperation with the media). Raising awareness will minimize the impact of the human factor as the weakest link in security[20].
- Improving cooperation and communication: It is recommended to establish formal channels for the exchange of information on incidents between the public and private sectors, e.g. by launching a national alert exchange platform accessible to operators of essential services and other interested companies. The state may also encourage the creation of industry-specific ISACs in sectors such as finance, energy, and transportation, where private entities jointly analyze threats. At the local government level, mechanisms encouraging the sharing of security specialists (e.g., a county employing an expert serving several nearby municipalities) should be considered.
- Regular audits and resilience tests: The government should finance and organize periodic cybersecurity audits of public institutions (especially at the local level) to detect and remove the weakest points. It is important that these audits are advisory rather than punitive in nature–the goal is to improve the situation, not to punish mistakes. At the same time, simulation exercises involving various entities (e.g., a nationwide exercise to respond to a massive ransomware attack on critical infrastructure) should be conducted to test procedures in conditions close to real life.
- Combating disinformation: As part of the state security system, capabilities to monitor and counter disinformation campaigns should be identified and developed. It is recommended that a permanent analytical group (including media experts, sociologists, psychologists, and IT specialists) be established to monitor narratives that threaten the country's information security. Its work should result in rapid corrections and statements issued by state authorities and cooperation with online platforms to limit the reach of harmful content (while respecting freedom of speech). In the long term, building social resilience through media

19 A. F. Ruggiero, T. D. Owusu & J. J. Staley, *Ransomware in local government: Risk factors…*, op. cit., pp. 183–191.

20 M. van Haastrecht, B. Yigit Ozkan, M. Brinkhuis & M. Spruit, *Respite for SMEs: a Systematic Review of Socio-Technical…*, op. cit., p. 2

education and the promotion of critical thinking is the best strategy for defending against disinformation.

- International coordination: Poland should continue to actively participate in EU and NATO initiatives on cybersecurity, share information on threats, and draw on the expertise of its allies. It is worth seeking to intensify regional cooperation (e.g. within the Visegrad Group or the Three Seas Initiative) on the exchange of information about attacks, as cyber campaigns often affect countries in our region simultaneously. In addition, it is recommended to organize joint international exercises and develop cybersecurity mutual assistance mechanisms in case of a serious incident exceeding the defense capabilities of a single country.
- The implementation of the above recommendations will strengthen the state's cyber resilience. It should be remembered that cyber threats will intensify with advancing digitization – the development of Smart Cities, 5G networks, and the Internet of Things increases the potential attack surface and poses new challenges for defenders[21]. Therefore, continuous improvement and adaptation of strategies is essential – cybersecurity is a process, not a state that can be achieved once and for all.

Summary

Cybersecurity in the 21st century is emerging as one of the pillars of national security, alongside traditional domains such as military defense and internal security. The analysis presented in this article shows that threats from cyberspace–attacks on critical infrastructure, ransomware, disinformation, and internal organizational vulnerabilities–have the potential to cause serious crises and destabilize the state. The experiences of recent years (both global and domestic) confirm that no modern country can ignore the issue of cybersecurity.

Poland has taken significant steps by creating a legal framework (the KSC Act, strategies) and institutions responsible for cybersecurity. Nevertheless, much remains to be done, especially at the level of practical implementation of objectives and strengthening the weakest links. Research on the state of cybersecurity in local governments points to the need to raise awareness, improve the implementation of policies and procedures, provide regular training, and improve cooperation between entities. a positive trend is the growing international and cross-sector cooperation–cyber threats are increasingly seen as a common challenge requiring a joint response. The main conclusion of the analysis is the need for an integrated approach to cybersecurity in the state strategy. This means simultaneously strengthening technical defenses, developing human competencies, improving laws and procedures, and building a broad coalition for a secure cyberspace–from the government, through the private sector, to a risk-aware civil society. Only such a holistic approach will

21 K. M. Hou, X. Diao, H. Shi, H. Ding, H. Zhou & C. de Vaulx, *Trends and challenges in AIoT/IIoT/IoT implementation*, Sensors 2023, No 23(11), p. 11.

effectively minimize the risk of cyberattacks and limit their impact, making the state more resilient to the challenges of the 21st century.

Ultimately, cybersecurity is a continuous process: it requires ongoing threat assessment, strategy adaptation, and rapid response to emerging new attack techniques. a state that treats cyberspace as an integral part of its security domain must invest in its protection as intensively as it does in traditional defense forces. The price of neglect in this area can be very high, as evidenced by statistics (annual increases in the number of incidents by tens of percent) and high-profile incidents in recent years. It can therefore be argued that ensuring national security in the 21st century is inextricably linked to ensuring cybersecurity. According to this thesis, all efforts to raise the level of cyber protection – legal, organizational, technical, and educational – are an investment in the broader security and stability of the state.

Bibliography

Ustawa z dnia 5 lipca 2018 r. *O krajowym systemie cyberbezpieczeństwa* Dz. U. 2018 poz. 1560 z późń. zm.

Ruggiero, A. F., Owusu, T. D., & Staley, J. J. (2022). *Ransomware in local government: Risk factors, vulnerabilities, and exploitation during a global pandemic*. Issues in Information Systems, 23(4).

Ali, H., Elzeki, O. M., & Elmougy, S. (2022). *Smart attacks learning machine advisor system for protecting smart cities from smart threats*. Applied Sciences, 12(13), 6473.

Baranovska, T., Savitskyi, V., Serbov, M., Stoliar, Y., & Krutik, Y. (2024). *The impact of cybercrime on state and institutional security: Analysis of threats and potential protection measures*. Economic Affairs, 69(Special Issue).

Chodakowska, A., Kańduła, S., & Przybylska, J. (2022). *Cybersecurity in the Local Government Sector in Poland: More Work Needs to be Done*. Lex Localis – Journal of Local Self-Government, 20(1),

Cortese, T.T.P.; Almeida, J.F.S.d.; Batista, G.Q.; Storopoli, J.E.; Liu, A.; Yigitcanlar, T. *Understanding Sustainable Energy in the Context of Smart Cities*: a PRISMA Review.Energies 2022, 15, 2382.

Fordoński, R., (2019) *WannaCry ransomware cyberattack as violation of international law* Uniwersytet Warmińsko-Mazurski, Studia Prawnoustrojowe (44)

Hossain, S. T., Yigitcanlar, T., Nguyen, K., & Xu, Y. (2024). *Understanding local government cybersecurity policy: a concept map and framework*. Information, 15(10).

van Haastrecht, M., Ozkan, B. Y., Brinkhuis, M., & Spruit, M. (2021). *Respite for SMEs: a systematic review of socio-technical cybersecurity metrics*. Applied Sciences, 11(15), 6909.

Hou, K. M., Diao, X., Shi, H., Ding, H., Zhou, H., & de Vaulx, C. (2023). *Trends and challenges in AIoT/IIoT/IoT implementation*. Sensors, 23(11), 5074.

Sophos. (2023). *The State of Ransomware in State and Local Government 2023*. Retrieved from Sophos News (news.sophos.com).

Terlecka-Maciejewska, M. (2024). *Cybersecurity in Polish security system*. Zeszyty Naukowe Politechniki Śląskiej, seria Organizacja i Zarządzanie, 198(2024).

https://sophos.com The State of Ransomware in State and Local Government 2023. Retrieved from Sophos News. – dostęp 27.04.2025 r.)

https://mazovia.pl/pl/bip/komunikaty/incydent-cyberbezpieczenstwa (dostęp 28.04.2025 r.)

About the Author

Dawid Kądzioła is a university lecturer and a PhD candidate at the University of Agriculture in Kraków. His academic interests include mechanical engineering, ergonomics, and machine design. He is a graduate of the Police Academy in Szczytno, majoring in Internal Security. His second field of scientific interest is cybersecurity in ICT systems. He is a certified Information Security Management System (ISO 27001) auditor and a cybersecurity officer for essential services in accordance with ISO 27001 and ISO 22301 standards. He also holds the title of Level II Cybersecurity Officer awarded by the Polish Institute of Internal Control. a police officer for over 22 years, he is currently affiliated with the Communication and IT Bureau of the General Police Headquarters in Warsaw.