SILESIAN UNIVERSITY OF TECHNOLOGY PUBLISHING HOUSE

SCIENTIFIC PAPERS OF SILESIAN UNIVERSITY OF TECHNOLOGY 2024
ORGANIZATION AND MANAGEMENT SERIES NO. 198

CYBERSECURITY IN POLISH SECURITY SYSTEM

Małgorzata TERLECKA-MACIEJEWSKA

SZPZLO Warsaw – Wawer; lek.mterlecka@gmail.com, ORCID: 0009-0009-7589-9237

Purpose: the aim of the article is to provide a broader context for the discussion on the significance and role of cybersecurity system in Poland. Cybersecurity is extremely significant for individual users, enterprises and entire countries. Cyberthreats might lead to serious consequences, for example data theft, loss of reputation, financial losses. They can be even dangerous for national security. Therefore, cybersecurity is an intrinsic element of the security system which needs to be constantly enhanced and adapted to the dynamically changing environment of threats.
Design/methodology/approach: the article is cross-sectional. The implementation of the goal is based on a critical analysis of literature.
Findings: the cross-sectional approach and literature review employed in this study have contributed to a comprehensive understanding of cybersecurity system in Poland.
Practical implications: effective cybersecurity has a fundamental meaning for the stability and national security of Poland. Providing protection against cyberthreats is crucial for maintaining the continuity of essential services, securing data protection and citizens' privacy, as well as for preventing potential disruptions in the functioning of economy and critical infrastructure.
Social implications: an effective cybersecurity system builds public trust and strengthens the position of Poland on the international area as a country capable of protecting its interests in the digital world. In the face of dynamically changing threats, continuous improvement and adaptation of the cybersecurity system remains necessary to tackle contemporary challenges and ensure long-lasting stability and national security.
Originality/value: this paper has provided an in-depth exploration of cybersecurity system in Poland the context of management.
Keywords: cybersecurity, security system, threats, cyberthreat, management.
Category of the paper: literature review.

Introduction

Cybersecurity has become a crucial element in the modern system of national security. In the era of dynamically developing information and communication technologies, an increasing number of cyberthreats and increasingly advanced cyberattacks, it is necessary to ensure protection against cybercrime both on the national and international level. Similarly to

other countries, Poland is undertaking a number of legal, organisational and operational actions aiming at enhancing cybersecurity. The present paper presents crucial legal, institutional and operational aspects connected with cybersecurity in the Republic of Poland, as well as a role of international cooperation, education and public or private partnerships in this area. Moreover, it draws attention to challenges and future paths of development for the cybersecurity system, which are essential for maintaining stability and national security in the face of dynamically changing cyberthreats.

”In 2023, the level of threats in cyberspace on a global scale continued to be high, which also resulted in a significant level of cyberthreats in Poland. The activity of various groups acting illegally in the digital world was on the rise, including hacktivists, cybercriminal groups of a gainful character and groups connected with other countries or even operating directly within the APT system. The proliferation of cyberattacks also resulted from new types of threats which had emerged thanks to the development of new technologies and their increasing availability. The rising level of cyberthreats in contemporary digital environment exerts an influence on everyday functioning of citizens, enterprises and state institutions, which is why the effective functioning of the National Cybersecurity System needs to be constantly improved” (Report, 2024).

Cybersecurity in a theoretical approach

In order to understand what cybersecurity means, it is necessary to present its definition. Cybersecurity is a complex of practices, technologies, processes and actions aiming at the protection of computer systems, networks, devices, programmes and data against attacks, damages or unauthorised access. In the era of digitalisation and global communication, cybersecurity plays a critical role in ensuring integrity, confidentiality and availability of information.

Addressing the issue of security, one should begin with paying attention to the following aspects: Data Protection, Risk Management, Threat Prevention, Incident Response, and Awareness and Education.

A key element in the area of cybersecurity is connected especially with Data Protection, i.e. with ensuring that data are stored, processed and transferred in a safe way which prevents them from being stolen, damaged or lost. Data Protection involves data encryption, employing access policies and regular security audits. Encryption secures the data in transmission and storage, access policies indicate who can gain access to the data, whereas security audits regularly check the systems in terms of potential gaps or infringements (https://ikmj.com, 2024). In turn, Risk Management consists in identifying, assessing and prioritising threats related to information security. It involves the implementation of relevant control measures

aiming at minimalizing the risk of cybernetic incidents. Threat Prevention consists in employing preventive measures such as firewalls, systems of detecting and preventing intrusions (IDS/IPS) and antivirus software. It is also important to update the systems and applications regularly in order to fill security gaps and provide protection against new threats. Incident Response means developing and implementing response procedures. It involves detecting, analysing and reducing the effects as well as restoring the normal functioning of the systems after an attack (Pilarski, 2022). Furthermore, it is important to create special teams responding to computer security incidents (CERT/CSIRT), which are responsible for quick and effective management of various incidents. In turn, Awareness and Education comes down to organising trainings and campaigns the aim of which is to raise users' awareness of cyberthreats and useful practices in the area of security. It is also supposed to promote safe habits such as using strong passwords, avoiding suspicious links or phishing e-mails.

Cybersecurity is extremely significant for individual users, enterprises and entire countries. Cyberthreats might lead to serious consequences, for example data theft, loss of reputation, financial losses. They can be even dangerous for national security. Therefore, cybersecurity is an intrinsic element of the security system which needs to be constantly enhanced and adapted to the dynamically changing environment of threats.

Cybersecurity plays an essential role in protection against the threats of the modern world, which are becoming increasingly advanced and common. At the time of digital transformation, when almost each and every aspect of social, economic and political life is dependent on information and communication technologies, cyberthreats can have serious and long-term consequences.

Present-day cyberthreats

Among present-day threats of cybersecurity one should mention the following ones: ransomware, phishing, DDoS attacks, data theft, information leakage, or threats connected with the Internet of Things (IoT).

Ransomware attacks are based on malicious software which blocks access to a victim's systems or data, demanding ransom for unblocking them. The examples of such attacks are WannaCry and NotPetya. They are extremely dangerous since they can paralyse functioning of companies, hospitals, government institutions and critical infrastructure, leading to huge financial losses and disruption in providing crucial services. In turn, phishing is a form of social engineering which consists in obtaining confidential information (e.g. logins, passwords) by posing as trustworthy entities, and in manipulating people in order to gain unauthorised access to systems or information (https://www.netia.pl, 2024). The importance of these techniques results from their effectiveness in breaking security, which may lead to identity thefts, financial

frauds or data compromising. DDoS attacks (Distributed Denial of Service) consist in sending a vast number of enquiries in order to overload servers or networks and, consequently, make them unavailable (https://blog.az.pl, 2024). Such attacks are dangerous since they can block access to online services, causing discontinuity in business operations, financial losses and collapse of confidence among clients. Data theft and leakage of information consist in unauthorised obtaining of confidential information such as personal, financial or commercial data. Such incidents could result in collapse of confidence among clients, financial penalties, and the stolen information can be used in further cyberattacks. Finally, threats connected with the Internet of Things (IoT) result from the fact that IoT devices are often not properly secured, which makes them vulnerable to attacks. Such threats should not be overlooked since taking control over IoT devices can lead to disruptions in the functioning of smart homes, cities or even industrial systems.

In the face of rising and increasingly more complex cyberthreats, cybersecurity is becoming fundamental for national security, economic stability and privacy protection. Its importance is going to grow with further technological advancements and global digitalisation.

Legal aspects of cybersecurity in Poland

A fundamental legal act in the field of cybersecurity in Poland is the National Cybersecurity System Act of 5 July 2018 (National Cybersecurity System Act, 2018). The act specifies the following aspects: organisation of the national cybersecurity system as well as tasks and duties of all entities included in the system; ways of exercising supervision and control regarding the application of the provisions of the act and a scope of the Cybersecurity Strategy for the Republic of Poland. The act also implements the regulations of the European Union NIS (Network and Information Security) Directive (Directive EU, 2016), issued in 2016 as the first EU legal act which was aimed at increasing the level of network and IT systems safety in the entire European Union. The directive obliged member countries to introduce legal and organisational measures in order to improve the ability to prevent, detect and respond to cybernetic incidents. The crucial elements of the NIS Directive involve:

- identifying operators of essential services: sectors such as energy, transport, banking, healthcare, as well as providers of digital infrastructure must be considered crucial for the functioning of society and economy;
- security requirements and reporting incidents: operators of essential services and providers of digital services must implement proper security measures and report serious cybernetic incidents to relevant state authorities;

– national and EU cooperation: each member state must establish the Computer Security Incidence Response Team (CSIRT) and National Cybersecurity Office, as well as be involved in a special Cooperation Group which facilitates the exchange of information and most effective practices on the European Union level.

The NIS Directive is a foundation for building a consistent and integrated cybersecurity system in Europe. It enhances protection against the rising threats in cyberspace.

The National Cybersecurity System Act defines the national cybersecurity system which is expected to ensure cybersecurity on the national level, including undisrupted provision of essential services and digital services, by means of achieving a proper level of security of information systems responsible for providing the above mentioned services and by ensuring the management of incidents (National Cybersecurity Act, 2018). The national cybersecurity system involves numerous entities, including: operators of essential services; providers of digital services; Computer Security Incidence Response Teams operating on the national level and led by the Head of the Internal Security Agency, the Minister of National Defence, and Scientific and Academic Computer Network – National Research Institute; cybersecurity teams operating in particular sectors; public finances institutions, research institutes; entities providing services in the field of cybersecurity; institutions relevant for cybersecurity issues.

At this point it is necessary to mention Resolution no. 125 of the Council of Ministers of 22 October 2019 on the Cybersecurity Strategy of the Republic of Poland for years 2019-2024 (Resolution no. 125, 2019), adopting the Cybersecurity Strategy of the Republic of Poland for years 2019-2024 appended to the aforementioned resolution. This document replaced the National Framework of Cybersecurity Policy of the Republic of Poland for years 2017-2022, established by virtue of Resolution no. 52 of the Council of Ministers of 27 April 2017 on the National Framework of Cybersecurity Policy of the Republic of Poland for years 2017-2022.

Institutions responsible for cybersecurity issues

Institutions responsible for cybersecurity issues include:

– for the energy sector – the minister responsible for energy issues;
– for the transport sector, excluding the subsector of water transport – the minister responsible for transport issues;
– for the sector of banking and financial markets infrastructure – Polish Financial Supervision Authority;
– for healthcare sector – the minister responsible for healthcare issues;
– for the digital infrastructure sector – the minister responsible for computerisation (National Cybersecurity Act, 2018).

A crucial role in coordinating actions in the field of cybersecurity in Poland is played by the Ministry of Digital Affairs, which consequently builds and develops the national cybersecurity system in order to ensure the protection of Polish cyberspace on a proper level. The Ministry in cooperation with its partners prepares documents and legal acts which are supposed to enhance and foster the national cybersecurity system. The Ministry of Digital Affairs also devised the above mentioned Cybersecurity Strategy of the Republic Poland for years 2019-2024. Moreover, due to the efforts of the Ministry, the provisions of the National Security Strategy and the Cybersecurity Strategy of the Republic of Poland for years 2019-2024 have been considerably harmonised. A special role among the organisational units of the Ministry is played by the Department of Cybersecurity which undertakes various actions, for example:

- determines quality goals for the cybersecurity of the Republic of Poland,
- shapes policies regarding the cyberspace of the Republic of Poland in cooperation with central government administration authorities and local self-government units;
- cooperates with state authorities and relevant Computer Security Incidence Response Teams (CSIRT) in terms of developing the ability to monitor and prevent incidents concerning the security of ICT systems, and fulfils tasks connected with the cooperation with CSIRT teams on the European level,
- monitors the process of implementing the provisions of strategic documents;
- devises, implements and reviews strategic documents with regard to cyberspace security issues,
- coordinates projects connected with preparing and updating the national cybersecurity strategy,
- prepares drafts of legal acts concerning the national cybersecurity system, suggests amendments to these acts and to other legal regulations regarding the protection of Polish cyberspace,
- represents Poland in international organisations, i.a. the Horizontal Working Party on Cyber Issues in the European Council, Cooperation Group established in the NIS Directive, Central European Cyber Security Platform.

The actions of the Ministry of Digital Affairs are aimed at ensuring effective protection of Polish cyberspace and increasing its resistance to present-day threats in the area of cybersecurity (Bógdał-Brzezińska, Gawrycki, 2003).

When it comes to institutions dealing with cybersecurity issues, it is also important to mention Computer Security Incidence Response Teams operating on the national level and led by the Head of the Internal Security Agency, the Minister of National Defence, and Scientific and Academic Computer Network – National Research Institute. These Teams cooperate with each other, with institutions dealing with cybersecurity issues and the minister responsible for computerisation, providing a consistent and complete risk management system on the national level, performing tasks in favour of preventing cyberthreats of a cross-sectoral and cross-border

character, and also ensuring the coordination of reported incidents (National Cybersecurity Act, 2018). The tasks of the Teams include:

- monitoring cyberthreats and incidents on the national level; estimating risk connected with a revealed cyberthreat and occurrent incidents, incl. conducting a dynamic risk analysis;
- conveying information about incidents and risks to the entities of the national cybersecurity system;
- issuing statements concerning identified cyberthreats;
- reacting to reported incidents.

Coordinating actions and enacting the government policy in terms of ensuring cybersecurity in the Republic of Poland are one of the responsibilities of the Government Representative for Cybersecurity who is appointed and recalled by the Prime Minister. The main duties of the Representative include:

- analysing and evaluating the national cybersecurity system on the basis of the aggregate data and indicators devised in cooperation with public administration institutions and institutions dealing with cybersecurity issues;
- controlling the process of risk management of the national cybersecurity system by the use of the aggregate data and indicators devised in cooperation with institutions responsible for cybersecurity issues;
- giving opinions about government documents, incl. drafts of legal acts which have an influence on the fulfilment of tasks in the cybersecurity area;
- implementing new solutions and initiating actions with regard to ensuring cybersecurity on the national level (National Cybersecurity Act, 2018).

One should also point out that the Council of Ministers' actions are supported by a special Board of Experts which is an opinion-giving and advisory body in cybersecurity issues.

An important role in the Polish cybersecurity system is also fulfilled by the Government Centre for Security which takes part in crisis management and cross-ministerial coordination in the area of cybersecurity in Poland. Its main task is to monitor, analyse and react to cyberthreats on the national level. The Government Centre for Security is a central contact point for different institutions and government bodies. It coordinates their activities in case cybernetic incidents occur. By means of information exchange and cooperation with different ministries, the Government Centre for Security guarantees an effective reaction to threats and minimalizes negative effects of cybernetic incidents for the country and its citizens (Trubalska, Wojciechowski, 2019) It also plays a crucial role in creating and maintaining safety in Polish cyberspace.

Finally, it is also worth paying attention to CERT Poland (Computer Emergency Response Team) which fulfils a central role in responding to cybernetic incidents in Poland. Its main task is to respond quickly and effectively to all incidents related to the security of information and

cybernetic infrastructure. CERT Poland collects, analyses and circulates information concerning threats. In addition, it provides technical and advisory support in case of cyberattacks. One of the key areas of CERT Poland's functioning is cooperation with a private sector. By working together with companies and organisations from the private sector, CERT Poland facilitates the exchange of information about threats, provides tools and clues regarding security and assists in responding to incidents. Thanks to such cooperation, the private sector can more effectively protect its resources and data against cyberattacks, which contributes to the overall enhancement of cybersecurity in Poland.

Summary

Summarising the topic of cybersecurity in the security system of the Republic of Poland, one should emphasise key legal, institutional and operational aspects, which overall form a complex system of protection from cyberthreats. The principal legal aspect is the *National Cybersecurity Act* of 2018 which can be considered as a foundation for the Polish system of cyberspace protection. The act implements the provisions of the NIS Directive and assigns duties to operators of essential services, providers of digital services and public sector entities. These regulations are aimed to ensure a high level of network and IT systems security by the use of risk management, responding to incidents and ensuring the continuity of operation.

The cybersecurity system in Poland is based on the cooperation between numerous institutions, among which the essential role is played by the Ministry of Digital Affairs and the Government Centre for Security. Another important element is the cross-ministerial cooperation that involves both public and private sector, which allows more effective threat prevention (Terlikowski, 2019).

As for the operational level, a crucial role is performed by actions connected with monitoring and analysing threats, designing and developing the National Cybersecurity System, and implementing systems of early warning and responding to incidents. Training courses and educational campaigns are an indispensable element of raising the awareness and competences in the cybersecurity area.

In order to successfully face cybersecurity challenges, it is necessary to constantly develop and adapt the system. The crucial directions and strategies which need to be taken into consideration are:

- investing in new security technologies such as advanced detection and reaction systems, artificial intelligence used to analyse threats;
- increasing the competences of specialists in cybersecurity by means of trainings, certifications and educational programs, as well as educating end users on basic safety rules;

- enhancing cross-sectoral cooperation, tightening public and private cooperation in the exchange of information about threats, establishing public and private partnerships, and participating in international initiatives and cooperation networks;
- updating legal regulations in order to adapt the rules to the changing environment of threats, incl. implementing new regulations concerning data protection, liability for security infringements and requirements for reporting incidents;
- developing and improving the National Cybersecurity System (Report, 2024).

Effective cybersecurity has a fundamental meaning for the stability and national security of Poland. Providing protection against cyberthreats is crucial for maintaining the continuity of essential services, securing data protection and citizens' privacy, as well as for preventing potential disruptions in the functioning of economy and critical infrastructure. An effective cybersecurity system builds public trust and strengthens the position of Poland on the international area as a country capable of protecting its interests in the digital world. In the face of dynamically changing threats, continuous improvement and adaptation of the cybersecurity system remains necessary to tackle contemporary challenges and ensure long-lasting stability and national security.

References

1. Bógdał-Brzezińska, A., Gawrycki, M.F. (2003). *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie.* Warszawa, p. 64.
2. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (Official Journal of the European Union 19.7.2016, L 194).
3. https://blog.az.pl/co-to-jest-atak-ddos-i-jak-sie-przed-nim-chronic/?gad_source=1&gclid=CjwKCAjwgdayBhBQEiwAXhMxtjQO6KXZXNvLmGFYetXKDDsx6kXbxu3Eog-6t84cX6J-512vclkCXBoC_OoQAvD_BwE&gclsrc=aw.ds, 9.04.2024.
4. https://ikmj.com/jakie-sa-cele-cyberbezpieczenstwa/, 9.04.2024.
5. https://www.netia.pl/pl/blog/phishing-co-to-jest-jakie-sprawia-zagrozenie, 9.04.2024.
6. National Cybersecurity System Act of 5 July 2018 (Journal of Laws from 2023, item 913), art. 3, 36, 41, chapter 8.
7. Pilarski, G. (2022). Wybrane aspekty cyberbezpieczeństwa w organizacji w zakresie analizy ruchu sieciowego. *Zeszyty Naukowe Pro Publico Bono, No. 1(1),* pp. 120-122.
8. Report of the Government Representative for Cybersecurity for the year 2023 (2024). Warsaw, pp. 7, 93-96.

9. Resolution no. 125 of the Council of Ministers of 22 October 2019 on the Cybersecurity Strategy of the Republic of Poland for years 2019-2024 (Monitor Polski from 30 October 2019, item 1037).
10. Terlikowski, T. (2019). Bezpieczeństwo cyberprzestrzeni wyzwaniem naszych czasów. System cyberbezpieczeństwa w Polsce (w świetle obowiązującego prawa). *Zeszyty Naukowe SGSP*, *No. 71/3*, p. 16.
11. Trubalska, J., Wojciechowski, Ł. (2019). *Cyberbezpieczeństwo jako element bezpieczeństwa państwa i ochrony prywatności obywateli.* Lubin: Innovatio Press, p. 38.