European Research Studies Journal
Volume XXVI, Issue 3, 2023

pp. 208-223

Cyber Protection Activities for Citizens in Poland Compared to the EU

Submitted 15/07/23, 1st revision 30/07/23, 2nd revision 11/08/23, accepted 10/09/23

Piotr Ładny[1]

Abstract:

Purpose: *The aim of the article is to present the legal solutions for cyber security in the European Union and in Poland, as well as to identify the cyber security challenges faced by individual countries, their institutions and society.*
Design/Methodology/Approach: *The article analyzes the activities undertaken at the national and international level to build IT security systems and assesses the activities in this area in Poland and Europe to date. Based on the data collected, the main obstacles to improving cyber security competence were identified, as well as proposals for action in the area under study. The research method adopted by the author is secondary research, based on the analysis of literature, research results and legal regulations on cyber security.*
Findings: *EU countries have taken a number of measures to increase security in this area, including the development of training programs and the construction of comprehensive educational programs on protection against cyber threats. Unfortunately, there is still a lack of cybersecurity education in Poland, especially for young people and seniors, groups that are particularly vulnerable due to lack of access to cybersecurity training provided by employers. Therefore, Poland should take more active measures to improve cybersecurity education, including through teacher training, the development of specialized educational programs, and the dissemination of knowledge on the safe use of new technologies. This is essential to ensure the digital security of institutions, businesses and citizens.*
Practical implications: *The critical conclusions presented in the article are a starting point for further research, including the education of those groups most exposed to digital threats, which will allow the development of a set of actions that will be necessary to increase the cyber security of citizens in Poland.*
Originality/Value: *The author pointed out the measures taken to raise the level of cyber security and the most important obstacles these measures face. The analysis of the problem points to the insufficient competence of citizens in the field of cyber security and the low effectiveness of educational programs to date, and the need for a stronger inclusion in the Polish cybersecurity system of active measures aimed at raising the level of digital competence among citizens, including competence in the area of digital security and resilience as key to the further development of the digital economy and digital society. The conclusions formulated in this article are a contribution to the discussion on building a comprehensive cyber security system in Poland.*

Keywords: *Internet, cybersecurity, regulations.*
JEL codes: *K4, L78, M15.*
Paper type: *Research article.*

[1]*Dr., University of Szczecin, Institute of Spatial Management and Socio-Economic Geography, piotr.ladny@usz.edu.pl;*

1. Introduction

Nowadays, as most of our private and professional life has moved to the virtual space, cyber security has become one of the most important issues for countries, businesses and citizens. With the development of information and communication technologies, the number of threats and attacks targeting companies, government institutions, providers of key services and infrastructure, but also individuals, is rapidly increasing. The need to ensure security in cyberspace is becoming a priority and one of the most important challenges facing all governments.

The responsibility for ensuring information security at the state level lies primarily with governments and the specialized state institutions they have established. They are responsible for creating and implementing appropriate policies and regulations to protect citizens and businesses from cyber threats. As part of these policies and regulations, states should establish IT security systems to protect the critical components that make up critical infrastructure, such as energy, telecommunications, or financial systems (Noja *et al.*, 2021; Do *et al.*, 2022).

However, cyber security is not just a matter for governments and state institutions. Today, an increasing part of social, economic and political life takes place in the digital world, making protection against cyber threats an important issue not only for states, but also for businesses, scientific institutions and citizens themselves, who need to be aware of the risks associated with the use of digital technologies and act responsibly to protect their personal data and privacy.

The concept of cyber security is widely and ambiguously defined. Numerous academic and popular studies describe the term in different contexts, for example, emphasizing the importance of technological solutions or referring to legal, organizational, economic, social, political and other issues that are inextricably linked to the creation of information security systems (Diakun-Thibault, 2014).

A definition related to technical aspects can be found in the Polish Law on the National Cyber Security System, according to which the concept means: "the resistance of information systems to actions that threaten the confidentiality, integrity, availability and authenticity of processed data or related services offered by these systems" (Ustawa o krajowym systemie cyberbezpieczeństwa, 2022).

More broadly, the term is described in the Regulation of the European Parliament and of the Council as “the activities necessary to protect network and information systems, the users of such systems, and other persons affected by

cyber threats" (Regulation (EU) 2019/881, 2019).

It is worth noting that cyber security issues are interdisciplinary and multidimensional and therefore require the collaboration of experts from different fields, such as computer science, law or social psychology. One of the biggest challenges in creating effective information security systems is the rapidly changing cybercrime landscape.

Attacks are increasingly complex and challenging, and cybercriminals are using more and more sophisticated tools and techniques to bypass defense mechanisms. In such a situation, it is necessary to constantly update and evolve security systems to keep up with the changing threats. Another challenge is to ensure the protection of citizens' personal data.

With more and more data being processed online, the risk of data theft and criminal use is increasing. In this context, it is important to put in place effective regulations to protect the privacy and personal data of Internet users. It is becoming even more important to ensure the protection of critical infrastructure.

Attacks on systems such as power plants, energy grids or transport systems can have disastrous consequences for society and the economy. It is therefore necessary to provide effective solutions to protect against attacks and to react quickly in the event of a threat.

International cooperation is also extremely important to ensure cyber security. As attacks on computer systems are often cross-border in nature and cybercriminals operate from the territory of other countries, it is important to establish international cooperation to combat cybercrime and to share information and best practices on cyber security.

Despite the increasing efforts directed at improving security, there are still major gaps in cyber security systems. Many of these are due to a lack of awareness and education of citizens about the risks associated with the use of modern technologies.

A lack of knowledge about how to use the Internet safely can lead to the disclosure of confidential information, clicking on suspicious links, downloading potentially dangerous programs and applications onto devices, and ultimately infecting devices with malware.

Therefore, it is extremely important to run educational campaigns to raise public awareness of cyber security. Raising digital awareness through effective education efforts will have a positive impact on the level of digital security, particularly in light of the growing number of Internet-connected devices that are increasingly being used in cyber attacks (Budziewicz-Guźlecka, 2019).

2. Key Cyber Security Regulations in the EU and Poland

The European cyber security system is based on a number of regulations aimed at ensuring a high level of protection against digital threats at Member State and EU level. One of the most important pieces of legislation comprehensively regulating cyber security is the Network and Information Systems Directive, adopted on 6 July 2016 (Directive (EU) 2016/1148, 2016). This directive requires EU Member States to create national cyber security strategies, establish a national NIS competent authority, and introduces security requirements for critical infrastructure such as the energy, transport or financial sectors.

The NIS Directive also introduces requirements for the provision of information on IT incidents to cognizant authorities, and sets out the obligations of so-called key service operators, digital service providers and public entities. The text of the directive is based on three pillars: the creation of capabilities in all Member States in the context of cyber security strategy; transnational cooperation, and national supervision of critical industries. After six years of the NIS Directive, in January 2023, the European Parliament revised the existing regulations by adopting a new directive, referred to as NIS2 (Directive (EU) 2022/2555, 2022).

The reason for the revision of the existing regulations was the increasing digitization and the evolution of cyber security threats (e.g., related to the increase in the number of digital service providers and their growing popularity (e.g., cloud services). It was also deemed necessary to expand the catalog of "critical" sectors of the economy in terms of cyber security.

The new regulations cover a much wider audience and introduce new obligations related to the provision of cyber security, with the main aim of harmonizing the list of entities to which cyber security obligations apply across the EU and increasing the possibility of enforcing these obligations through the possibility of imposing financial penalties.

In addition to the NIS/NIS2 Directive, the Cyber Security Act (CA) is the regulation that lays the foundation for the European cyber security system (Regulation (EU) 2019/881, 2019). The Cyber Security Act was published on 7 June 2019 as part of the so-called cyber security package. It was the second pan-European cyber security regulation after the NIS Directive. The CA is divided into two parts. The first concerns the activities of ENISA, the European Network and Information Security Agency.

It was already established in 2004, under a previous law that regulated its activities (Regulation (EC) No 460/2004, 2004), but the evolution of threats in the area of IT security made it necessary to strengthen ENISA's competences, clarify the scope of its activities and expand its responsibilities to new areas. The Agency's main tasks are to coordinate cyber-security activities at European

level, to develop and promote best practices in cyber security, and to provide technical and advisory support to EU Member States on protection against cyber threats.

Through its activities, the Agency supports the process of creating effective cyber security solutions for the European Union Member States and other EU bodies (Gawkowski, 2018). The second part of the CA creates a cyber security certification framework for ICT products and services. The regulation establishes a mechanism for setting up European cyber security certification programs and for confirming that products or services meet certain security requirements.

The goal is to ensure that devices and solutions that have been tested and meet the relevant security standards reach the market. With the certification recognition scheme, companies do not have to apply for certification in every country where they want to offer their services or products.

As the financial sector becomes increasingly reliant on digital software and processes, making it vulnerable to cyberattacks, the European Parliament adopted the Digital Operational Resilience Act (DORA) in November 2022. DORA is an EU regulation that aims to establish a single and comprehensive framework for the operational digital resilience in the financial sector.

Financial market operators must implement solutions to effectively respond to and combat all types of disruptions and risks related to information and communication technologies. The new rules apply to all financial services firms – including banks, payment service providers, e-money institutions, investment firms, cryptocurrency service providers, and critical external ICT service providers (Regulation (EU) 2022/2554, 2022).

An extremely important piece of legislation in the EU information security regime is also the General Data Protection Regulation (GDPR), which regulates the processing of personal data by companies, institutions and organizations in the European Union (Regulation (EU) 2016/679, 2016).

The GDPR aims to ensure the privacy and protection of this data, forcing data processors to put in place appropriate safeguards and protections. Unlike the NIS/NIS2 Directive, which focuses on the security of networks and information systems, the GDPR addresses issues related to the security of personal data (Hydzik, 2019).

The cyber security system in Poland is largely based on the implementation of EU regulations, and the most important legal acts that define the obligations of both state bodies and private entities in terms of protection against IT threats include:

1. The Act on the National Cyber Security System (Ustawa o krajowym systemie cyberbezpieczeństwa – UoKSC) – sets out the principles for the functioning and organization of the cyber security system in Poland, including the role of state bodies responsible for ensuring the security of IT networks and systems, and is the first piece of legislation in Poland to regulate cyber security in a horizontal manner. The Act is a transposition of the so-called NIS Directive into national law, and primarily regulates the so-called key service operators, which are subject to very restrictive cyber security obligations (Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, 2022);

2. The Personal Data Protection Act (Ustawa o Ochronie Danych Osobowych – UoODO) defines the principles of personal data processing and the rights of data subjects (data subjects). It provides the legal basis for the protection of privacy and the protection of personal data. The law aims to ensure that the processing of personal data is carried out in accordance with the principles of lawfulness, transparency, purposefulness and limitation of data processing, and with respect for the rights of data subjects (Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, 2018). Due to the fact that the EU GDPR Regulation is a legal act that is directly applicable in all Member States, the Polish act only details certain issues (e.g. the procedure for the appointment of a Personal Data Inspector, the principles of accreditation and certification, or the powers of the President of the Office for Personal Data Protection);

3. The Act on Informatization of the Activity of Entities Performing Public Tasks (Ustawa informatyzacji działalności podmiotów realizujących zadania publiczne – (UoIDPRZP) – contains provisions on the computerization of public administration activities and requirements for the security of IT systems (Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, 2005).

Due to the increasing number of threats related to cybercrime, hacking attacks or data leaks, government and regulatory bodies at EU, national and international levels are paying more attention to the issue of cyber security. As part of this process, extensive measures are in place to reduce the risk of cyber threats and minimize their impact.

In addition to the legislation mentioned above, cyber security strategies are also being developed and other activities are being undertaken that involve government and regulatory bodies are involved in creating appropriate structures and standards, implementing regulations and providing technical and training support.

As a result, government and regulatory bodies are playing an increasingly

important role in developing and implementing effective cyber security solutions to protect against threats to society, business, and critical infrastructure.

3. Digital Threats and Cyber Defense Competences of Polish and EU Citizens

The development of the Internet, with the emergence of new technologies and new services and the increase in the number of users, brings both benefits and risks. Globally, the number of people using the Internet is growing every year. In January 2023, the total number of Internet users exceeded 5.1 billion, which means a penetration of 64.4% (Data Breach Investigations Report, 2022). In Poland, it is estimated that at the beginning of 2023, the number of Internet users will reach 36.68 million, with a penetration of 88.4% (Digital 2023; Poland, 2023).

As the number of users increases, so does the volume of Internet user activity and the number of devices connected to the network. The total number of such devices in the world in 2022 has been estimated at more than 15 billion, with technological development, including in particular the development of the so-called Internet of Things (IoT), expected to contribute to the rapid growth of this number in the coming years. According to Strategy Analytics, there will be 38.6 billion Internet-connected devices in three years and 50 billion in five years (Global Connected and IoT …, 2023).

In practical terms, this means that the number of potential targets for cyberattacks and the number of people and companies affected by various IT incidents is increasing every year. The cost of dealing with incidents is also rising rapidly. Cyber Security Ventures, a cyber security research center, estimated that the costs generated in this way for the global economy in 2021, reached US$6 trillion, compared to around US$3 trillion just 10 years ago. By 2026, total spending on securing networks and services is expected to be as high as $16.8 billion (Cybercrime To Cost …, 2023).

Analyses and reports on cyber security indicate that the number of digital threats and cyberattacks has increased worldwide in recent years, including in European countries. This increase affects not only the number, vectors, and means of attacks or the areas affected by the threats, but also their impact on users and economic systems. Geopolitics and international conflicts are leading to an increase in government-sponsored attacks, including on critical sectors of the economy. Disinformation spread through digital communication channels (including social media) is also a growing threat.

Large enterprises and critical infrastructure operators are not alone in facing these threats. According to Verizon's 2022 Data Breach Investigations Report, 43% of cyberattacks today target small businesses rather than large enterprises

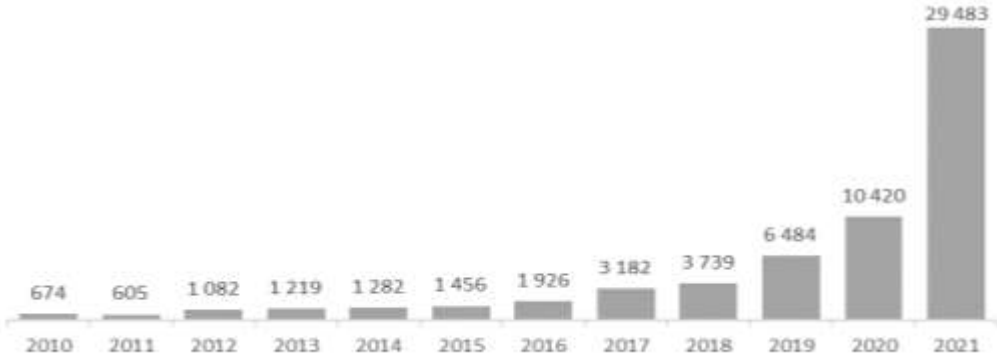
(Data Breach Investigations Report, 2022. According to an EU study published in May 2022, 28% of European SMEs were victims of cybercrime in 2021 (SMEs and Cybercrime …, 2022), and Checkpoint estimates that the number of cyberattacks on corporate networks increased by 50% in 2021 compared to 2020 (Check Point Software's 2022 Security Report, 2022). The total number of unique cyber threats detected in 2021 is estimated to have increased by 36.5% compared to 2020 (Moyal, 2022).

The most common types of threats in 2022, according to ENISA, include ransomware, malware, social engineering, threats to data, threats to availability: denial of service, threats to availability: Internet threats, disinformation (misinformation) threats, and supply chain attacks. The European Union Agency for Cyber Security estimates that the cost of dealing with a security incident in the EU is typically between €213,000 and €300,000 and, taking into account the number of detected attacks and incidents, the most vulnerable sectors include (ENISA Threat Landscape 2022, 2022):

1. public administration/government (24% of reported incidents),
2. digital service providers (13% of reported incidents),
3. general public (12.4% of reported incidents),
4. services (11.8% of reported incidents),
5. finance/banking (9% of reported incidents)
6. healthcare (7% of reported incidents).

The increase in IT threats and incidents is also observed in Poland. CERT Polska - Poland's first computer incident response team, which has been part of the national cyber security system since 2018 - reported that it registered and handled a total of 29,483 unique cyber security incidents in 2021. This represents a 182 percent increase in the number of incidents handled compared to 2020 (Krajobraz bezpieczeństwa polskiego Internetu, 2021). The number of incidents handled between 2010 and 2021 is shown in Figure 1.

Figure 1. *Number of incidents handled by CERT Polska in 2010-2021*



Source: *Own study based on data from CERT Polska.*

Taking into account the number of incidents recorded by CERT, the most popular type in 2021 was phishing – accounting for as much as 76.57% of all incidents handled. The number of incidents classified as phishing compared to the previous year increased by 196%.

The second type of incident in terms of number of submissions was malware. This type of incident was 28% higher in 2021 than last year. Third place in the ranking of the number of incidents registered last year goes to the category of offensive and illegal content, including spam. The percentage of this type of incident was 1.05%. Such a small percentage is due to the fact that CERT Polska often attributes multiple submissions to a single incident. This is particularly noticeable for this category of incidents, where as many as 21,522 submissions were responsible for 311 incidents (Krajobraz bezpieczeństwa polskiego Internetu …, 2021).

The development of cyber threats means that the problem of ICT security affects not only companies and public entities, but also becomes a challenge for citizens. A survey commissioned by the European Commission at the end of 2019 shows that, on average, a quarter of all respondents know someone who has received emails or phone calls in the past three years aimed at phishing for personal or access data, while around 21% of respondents know someone who has detected malware on their device.

At least 13% of respondents have experienced online fraud, hacking into a social networking or email account, or who has been a victim of bank card or online banking fraud (10%). The respondents also cited threats such as identity theft, harassment or cyberbullying.

The percentage of respondents who had personally experienced security incidents was 36% in the case of emails or phone calls aimed at phishing for personal or access data, around 28% had discovered malware on their device, 13% indicated that they had encountered hate or extremist content and 11% of respondents had experienced the hijacking of social media accounts or email accounts.

It is noteworthy that the percentage of each response varied depending on the country in which the survey was conducted. For example, the highest number of people who personally experienced a malware infection was in Austria and Luxembourg (40%) and the lowest in Portugal (11%) (Europeans' attitudes towards …, 2020).

The vast majority of respondents (76% on average) perceived a growing risk of becoming a victim of cybercrime (in Poland – 72%), 68% were concerned about the security of personal data collected and processed by websites and more than 61% were convinced that they do not guarantee the security of their personal

data. The increased feeling of insecurity is also confirmed by research conducted in Poland.

The results of a consumer survey conducted by ING bank show that 70% of Poles notice an increase in threats and attacks, and more than 80% are concerned about online safety, which may be related not only to the increasing amount of information about cyber security, but also to the fact that 44% of respondents have experienced or know someone who has experienced a cybercrime. More than half of the respondents also confirmed familiarity with at least some cyber threats – phishing, malware and online fraud were among the most commonly cited (more than 60%) (Polacy i cyberbezpieczeństwo …. 2022).

Of particular importance in the context of the survey results presented here is the fact that, despite respondents' increasing awareness and sense of threat, their belief that they have sufficient skills to protect themselves from threats is declining. Only 59% of Europeans believe they have sufficient knowledge and skills to protect themselves against this type of crime (down from 71% in 2017). Of the 28 countries surveyed, there are only 15 where more than half of the citizens believe they are able to protect themselves effectively enough against cyber threats. The highest percentages are observed in the UK (73%), Denmark (67%) and Finland (66%).

At the other end of the scale are countries such as Bulgaria (30%), Greece (36%) and Lithuania (40%). Poland is slightly above average among the countries surveyed, with a score of 53%. The lack of knowledge about what to do in a threatening situation is also confirmed by the fact that only one in five respondents (22% on average) said they knew of an official channel for reporting cybercrime (website, e-mail address, online form or contact number) or other illegal behavior on the Internet (20% in Poland).

Nearly 80% of respondents do not know how and where to report cyber threats (SMEs and Cybercrime …, 2022). The results of ING's survey confirm the low level of knowledge about cybercrime procedures. Only 14% of respondents indicated they knew very well what to do in such a situation, while 43% had no such knowledge at all (Polacy i cyberbezpieczeństwo …, 2022).

According to a study conducted by CBM Indicator on behalf of Google (Jesteśmy coraz bardziej świadomi zagrożeń w sieci, 2022), almost two-thirds of Poles can be classified as digital newbies. This is a group of people who are insufficiently competent to move safely on the Internet, are not aware of the threats lurking on the Internet, do not know how to defend themselves against them and how to react to them. Up to 56.9% of Polish Internet users belong to this group. They are mainly people over 55 years of age, and pensioners account for about a third of this group (29.7%).

The lack of sufficient knowledge in the field of cyber security is part of a broader phenomenon in Poland – the low level of digital literacy in the broadest sense. These competences are necessary to build information societies, i.e., societies in which information leads to the transformation of all areas of socio-economic life (Aftański, 2011), but in Poland they are still at a lower level than in other European countries and the average for these countries. Lack of digital competences, fear of using the Internet, lack of or insufficient motivation, lack or insufficient skills contribute to the deepening of digital exclusion in society (Budziewicz-Guźlecka and Drab-Kurowska, 2020).

Taking into account digital literacy at both basic and advanced levels, two of the elements on the basis of which the Digital Economy and Society Index (DESI) is based, it can be seen that Poland ranks among the 4 worst EU countries, ahead of only Italy, Bulgaria and Romania (The Digital Economy and Society Index, 2022).

4. Discussion

Data from Eurostat and the 2021 DESI report show that 39% of EU citizens who used the Internet in 2019 experienced security problems. Incidents such as data security breaches, online fraud or data leaks have serious consequences not only for companies and institutions, but also for citizens. More and more cyber security initiatives are being taken at international and national levels.

However, it should be noted that the security system developed so far has focused on selected areas such as the protection of critical infrastructure, the fight against terrorism, the fight against economic crime, etc. Cyber security regulation has mainly concerned large market players and public institutions.

Much less emphasis has been placed on the security of citizens and their protection from cyber threats. While companies, public institutions or social organizations often have the knowledge, prepared staff and systemic support, it is the "ordinary" citizen who seems to be the most vulnerable entity and who finds it most difficult to take effective measures to limit the scale of losses caused by crime and to reduce the risks associated with operating in cyberspace.

While, at the EU level, this problem is reflected in programs and strategies aimed at developing learning and training opportunities that will increase awareness of cyber security, in Poland, action in this area is insufficient and delayed. A report published in November 2022 by the Polish Supreme Audit Office (Najwyższa Izba Kontroli – NIK) indicates that the national cyber security system being developed in Poland in practice ignores the largest group of Internet users, i.e. individuals, and focuses attention on strengthening the security of systems considered crucial for the functioning of the state (Działania Państwa w zakresie …, 2022).

Although the police is considered by the majority of Internet users to be the authority responsible for reporting cybercrime, its units lack the proper procedures and algorithms to deal with such cases. Another problem is the lack of sufficient human, financial and equipment resources necessary to perform the tasks of preventing and minimizing the effects of Internet crime.

As of December 2021, there were only 305 officers (338 persons, including civilian employees) employed in the Cybercrime Department of the Police in Poland, which is only 0.33% of all full-time positions in the police.

According to the results of the questionnaire survey conducted by the SAO, as many as 85% of the persons who were victims of computer crimes and reported them to the police received no explanation, the case was dropped, or money and data were lost. On the other hand, only 2% of cases resulted in the detection and conviction of the perpetrator or the recovery of lost funds.

The establishment of the Central Office for Combating Cybercrime within the police structures in January 2022 and the activities of the CSIRT of NASK in the area of incident handling and victim support should be considered as an element of positive change. However, the lack of specialists in the field of combating cybercrime remains a problem. The results of the survey also indicate a lack of knowledge about the possibility of obtaining support from the NASK (only 1% of respondents stated that they were aware of this issue).

The SAO's report assesses as insufficient and ineffective the measures taken to educate and warn citizens about the dangers they face from the perpetrators of online crimes. Although the need for cyber security education at the primary school level is now highlighted as a key element, Poland lacks a harmonized system for building citizens' competence in this area. Curricula currently do not specify the scope of knowledge that should be taught at different levels of education and the methods of validating this knowledge.

The actions of the Ministry of Education and the Ministry of Digitalization in this regard have so far been mainly conceptual. In August 2022, curricular changes were introduced in the subject of education for security, which included cyber security among the topics to be taught in this subject.

However, it should be noted that this is only an additional element in the curriculum of this subject. An additional problem in the implementation of these courses in the near future may be the lack of adequately prepared personnel, who not only need to have the appropriate knowledge, but also need to update this knowledge in accordance with the dynamic changes taking place in the field of cyber security.

In February 2023, the Council of Ministers adopted a resolution to establish a

Digital Competence Development Program with a budget of more than PLN 2 billion 789 million. The aim of the program, which will run until 2030, is to increase the level of digital literacy in society and to develop digital education. Although the goal of this program is not in doubt, the detailed regulations are criticized by experts as inconsistent and incomplete (Opinia na temat …, 2023).

A good example of the creation of a comprehensive framework for the cyber security education process can be found in the European Digital Europe (DIGITAL) program and a 3-year project implemented in Finland from September 2022 under the auspices of the Ministry of Transport and Communications and Aalto University, which aims to develop an educational package to support cyber security education in EU Member States.

The implementation of this project is funded by the EU's Recovery and Resilience Facility, which is aimed at rebuilding the economy after the coronavirus pandemic. Poland will be the fourth largest beneficiary of this facility, and 20% of the total amount of support Poland will receive is earmarked for digitalization, including cyber security activities. The condition for receiving these funds is that Poland submits a national recovery plan, which it has not yet done due to the failure to meet the conditions of the European Commission.

5. Conclusion

The increase in threats associated with the use of modern technologies and the growing awareness of citizens and decision-makers in this area have contributed to the increased activity of European Union countries to improve digital security.

The data presented shows that the number of attacks on information systems, including companies, public institutions and citizens, is steadily increasing, making the challenges of building digital security systems ever greater. EU countries have taken a number of measures to increase security in this area, including the development of training programs and the construction of comprehensive educational programs on protection against cyber threats.

Unfortunately, there is still a lack of cybersecurity education in Poland, especially for young people and seniors, groups that are particularly vulnerable due to lack of access to cybersecurity training provided by employers. In addition, the use of the Internet and mobile devices has become commonplace for children and young people, and digital security knowledge is essential to using these tools wisely and avoiding risks.

The importance of this knowledge increases with entry into the labor market, as many employers require their employees to be able to use various digital tools in a safe manner. Therefore, Poland should take more active measures to improve cybersecurity education, including through teacher training, the development of

specialized educational programs, and the dissemination of knowledge on the safe use of new technologies. This is essential to ensure the digital security of institutions, businesses and citizens.

These issues are a starting point for further research, including the education of those groups most exposed to digital threats, which will allow the development of a set of actions that will be necessary to increase the cyber security of citizens in Poland.

References:

Aftański, P. 2011. Społeczeństwo informacyjne – nowy wymiar informacji. Dydaktyka informatyki, 6, 66-73.

Budziewicz-Guźlecka, A., Drab-Kurowska, A. 2020. Problems of Infrastructure Markets with Particular Emphasis on the Postal Market in the Context of Digital Exclusion. Sustainability, 12, 4719, 2.

Budziewicz-Guźlecka, A. 2019. Oddziaływanie polityki społeczno-gospodarczej na zmiany polskiego rynku usług telekomunikacyjnych. Wydawnictwo Naukowe Uniwersytetu Szczecińskiego, 248.

Check Point Software's 2022 Security Report. 2022. Available at: https://pages.checkpoint.com/cyber-security-report-2022.

Cybercrime To Cost The World 8 Trillion Annually in 2023. 2023. Available at: https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023.

Data Breach Investigations Report. 2022. Available at: https://www.verizon.com/business/resources/reports/ dbir.

Diakun-Thibault, N. 2014. Defining Cybersecurity. Technology Innovation Management Review, 2014, 13-16.

Digital 2023: Global Overview Report - DataReportal – Global Digital Insights. 2023. Available at: https://datareportal.com/reports/digital-2023-global-overview-report.

Digital 2023: Poland. 2023. DataReportal – Global Digital Insights. Available at: https://datareportal.com/reports/digital-2023-poland.

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. EP, CONSIL, 194 OJ L 194 (2016).

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), OJ L 333 (2022).

Do, T.D., Pham, H.A.T., Thalassinos, I.E.., Le, H.A. 2022. The impact of digital transformation on performance: Evidence from Vietnamese commercial banks. Journal of Risk and Financial Management, 15(1), 21.

Działania Państwa w zakresie zapobiegania i zwalczania skutków wybranych przestępstw internetowych, w tym kradzieży tożsamości. (KPB.430.010.2022). 2022. Najwyższa Izba Kontroli. Available at: https://www.nik.gov.pl/aktualnosci/przestepstwa-internetowe-zapobieganie-i-

zwalczanie.html.
ENISA Threat Landscape 2022. 2022. (Report/Study). Available at: https://www.enisa.europa.eu/ publications/enisa-threat-landscape-2022.
Europeans' attitudes towards cyber security (cybercrime) - Eurobarometer survey. 2020. Available at: https://europa.eu/eurobarometer/surveys/detail/2249.
Gawkowski, K. 2018. Bezpieczeństwo cyberprzestrzeni w regulacjach UE. Teka Komisji Politologii i Stosunków Międzynarodowych, 13(2), 69.
Global Connected and IoT Device Forecast Update. 2023. Available at: https://www.strategyanalytics.com/access-services/devices/connected-home/consumer-electronics/reports/report-detail/global-connected-and-iot-device-forecast-update.
Hydzik, W. 2019. Cyberbezpieczeństwo i ochrona danych osobowych w świetle regulacji europejskich i krajowych. Przegląd Ustawodawstwa Gospodarczego, 3, 86.
Jesteśmy coraz bardziej świadomi zagrożeń w sieci. 2022. Available at: https://polska.googleblog.com/2022/11/jestesmy-coraz-bardziej-swiadomi.html.
Krajobraz bezpieczeństwa polskiego Internetu w 2021 roku. 2021. Available at: https://cert.pl/uploads/docs/Raport_CP_2021.pdf.
Moyal, M. 2022. 2021 State of Cybersecurity Effectiveness Usage Report. Available at: https://cymulate.com/resources/2021-cybersecurity-effectiveness.
Noja, G.G., Cristea, M., Thalassinos, E., Kadłubek, M. 2021. Interlinkages between Government Resources Management, Environmental Support, and Good Public Governance: Advanced Insights from the European Union. Resources, 10(5), 41.
Opinia na temat „Programu Rozwoju Kompetencji Cyfrowych do roku 2030". 2023. Sektorowa Rada ds. Kompetencji. Telekomunikacja i Cyberbezpieczeństwo. Available at: https://srtcb.radasektorowa.pl/publikacje-raporty/badania-i-analizy/369-opinia-dot-programu-rozwoju-kompetencji-cyfrowych-do-roku-2030.
Polacy i cyberbezpieczeństwo - Raport. 2022. Available at: https://spolecznosc.ing.pl/-/Blog/Raport-Polacy-i-cyberbezpiecze%C5%84stwo-Om%C3%B3wienie-najciekawszych/ba-p/39787.
Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency. OJ L 077 (2004).
Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). OJ L 119 (2016).
Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). OJ L 151 (2019).
Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011. OJ L 333 (2022).
SMEs and Cybercrime—Eurobarometer survey. 2022. Available at: https://europa.eu/eurobarometer/surveys/ detail/2280.
The Digital Economy and Society Index (DESI). 2022. Available at: https://digital-

strategy.ec.europa.eu/pl/policies/desi.

Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, nr Dz.U. 2018 poz. 1000. 2018. Available at: https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001000.

Ustawa z dnia 17 lutego 2005 r. O informatyzacji działalności podmiotów realizujących zadania publiczne, nr Dz.U. 2005 nr 64 poz. 565. 2005. Available at: https://isap.sejm.gov.pl/isap.nsf/ DocDetails.xsp?id=wdu20050640565.

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, nr Dz.U. 2022 poz. 1863, ze zm. 2022. Available at: https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001560.