BEZPIECZEŃSTWO TEORIA I PRAKTYKA SECURITY THEORY AND PRACTICE
e-ISSN 2451-0718
ISSN 1899-6264
2021
No. 1 (XLII)

DOI: 10.48269/2451-0718-btip-2021-1-012
Received: 14.12.2020
Accepted: 30.03.2021

Karol Piękoś

University of Rzeszów
https://orcid.org/0000-0003-4545-5909

Actions taken to protect the cyberspace of the Republic of Poland in the years 2015–2019

Introduction

Cyberspace has been defined in a variety of ways. One of the approaches to the notion recommends regarding it as a communication space created by internet connection systems. Cyberspace users can communicate and relate in real time. Today, from the military point of view, cyberspace is treated in the same way as the marine, land, air and space environment. The major features of cyberspace include anonymity, anti-territoriality, global scope, and regularity.[1] Representatives of states and international organisations have repeatedly emphasised that it is necessary to develop specific defence capabilities in cyberspace given the scale of threats. Many countries strive to build offensive capabilities in cyberspace with the use of various methods.[2] Security in cyberspace is often defined as the lack of risk of losing information data, which is an important element of civilisation progress and development. In this area, the information collected there is protected. Information security in cyberspace is an integral part of national security.[3]

1 M. Marczyk, 'Cyberprzestrzeń jako nowy wymiar aktywności człowieka – analiza pojęciowa obszaru', *Przegląd Teleinformatyczny*, Vol. 6, No. 1–2, 2018, pp. 59–60.

2 M. Grzelak, K. Liedel, 'Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu', *Bezpieczeństwo Narodowe*, No. 22, 2012, p. 128.

3 T. Terlikowski, 'Bezpieczeństwo cyberprzestrzeni wyzwaniem naszych czasów. System cyberbezpieczeństwa w Polsce (w świetle obowiązującego prawa)', *Zeszyty Naukowe SGSP*, No. 3 (71), 2019, p. 85.

In the years 2015–2019, i.e. during the 8th term of the Sejm of the Republic of Poland, the parliamentary majority was in the hands of the United Right, headed by the Law and Justice party (Prawo i Sprawiedliwość, PiS), which had secured 235 seats in the Sejm. During the election campaign in 2015, cybersecurity did not play a major role. The 2014 political manifesto of Law and Justice included numerous references to the notion of national security, but cybersecurity appeared only in the context of allied guarantees, and the need to defend the country against modern threats also in this dimension.[4]

Although cybersecurity has been discussed many times in the public debate in the context of hacking attacks on public institutions and enterprises, in the first decade of the twentieth century it did not constitute a particular point of interest among politicians. Despite the marginal role in the political discourse, threats originating from the Internet have continued to play a pivotal role in the security of the state. Already before 2010, it was pointed out that attacks using the ICT infrastructure had become a form of terrorist activity, and Poland – given its participation in military operations in Iraq and Afghanistan – could become an object of interest for cybercriminals as well. The growing percentage of the world population using the Internet on their mobile devices has also increased interest in Poland among the countries and organisations that can launch attacks online. The cooling down of the relations with the Russian Federation, which in the international community has been suspected of increased activity in the field of cyberespionage and cyberterrorism, could also become the cause of potential threats in the years to come.[5]

There have been numerous hacker attacks all over the world in the twenty-first century. On 22 January 2012, Anonymous Group posted a message on Twitter, heralding the beginning of the "Polish Revolution." The goal of this step was to oppose the *Anti-Counterfeiting Trade Agreement* (ACTA).[6] Hackers' actions caused many websites to stop working, including the official website of the Sejm, the Prime Minister's Office, the President's Office, the Central Bureau of Investigation, and numerous government departments. The situation was serious and had a real impact on the perception of cyber threats by the politicians in power.[7] Similar actions also took place in other countries, such as the massive attacks on government servers in Estonia in 2007. The political conflict resulted in one of the largest cyber-attacks, which posed a real threat to state security. The situation was serious, and support in the field of cybersecurity was provided to Estonians by NATO network security experts.[8]

---

4 Program Prawa i Sprawiedliwości 2014, p. 162, http://pis.org.pl/dokumenty?page=2 [accessed: 10.12.2020].

5 M. Łapczyński, 'Zagrożenie cyberterroryzmem a polska strategia obrony przed tym zjawiskiem', *Komentarz Międzynarodowy Pułaskiego*, No. 7, 2009, pp. 3–4.

6 ACTA was a multilateral agreement aimed at regulating international standards for combating infringements of intellectual property. Due to public opposition across Europe, there were mass protests in which participants demanded the rejection of ACTA.

7 J. Bolanowski, 'Protest przeciw ACTA, atak hakerów Anonymous, czyli powstanie styczniowe w Internecie', https://forsal.pl/artykuly/586784,protest-przeciw-acta-atak-hakerow-anonymous-czyli-powstanie-styczniowe-w-internecie.html [accessed: 10.12.2020].

8 S. Wierzbicki, 'Wojny cybernetyczne jako element niekonwencjonalnej konfrontacji międzypaństwowej. Pragmatyczna rzeczywistość, nieunikniona przyszłość', *De Securitate et Defensione*, No. 2(1), 2015, pp. 141–142.

One of the underlying goals of the paper is to verify the research hypothesis according to which the role of cybersecurity in Poland has increased in the period scrutinised in relation to the previous years. In order to verify it, the following questions were pondered: 1) What actions were taken to protect cyberspace in Poland in 2015–2019? 2) Did international organisations have any impact on the Polish government to make additional efforts to improve the country's security on the Internet? 3) What threats to cyberspace security appeared in Poland during the eighth term of the Sejm of the Republic of Poland?

Of the research techniques used to write the paper, institutional-legal analysis has taken the lead, as it has allowed for the study of legal norms that determine the functioning of state authorities and institutions in the field of cybersecurity,[9] along with the comparative method, which has been applied to confront the state of cybersecurity in the various periods subjected to scrutiny.[10]

Protection of Polish cyberspace before 2015

Mentions of cyberspace protection in Poland first appeared in academic publications as early as in the 1980s and the 1990s. At that time, attention was paid to the potential threats that may arise in connection with the use of computer networks.[11] In 1996, within the Scientific and Academic Computer Network (NASK), the Computer Emergency Response Team (CERT) was established in Poland, which was a team aimed at responding to network security incidents.[12] In 2008, CERT.GOV.PL – the Governmental Computer Response Team – was set up to address a number of similar issues. Since 2008, within the Ministry of the Interior and Administration (MSWiA) and, *inter alia*, at the Internal Security Agency (ABW), several actions have been taken to devise a national strategy for counteracting the dangers that appear in cyberspace. Taking steps to develop a strategic document resulted from the development of the Internet and progressive computerisation, which has created many opportunities and threats – mostly given the potential threat of using the network for cyber-attacks.

The key tasks of CERT.GOV.PL included: 1) creating a policy in the field of protection against cyber threats; 2) coordinating the flow of information between entities in this field; 3) detection, identification and prevention of cyber threats; 4) cooperation with national institutions, organizations and departmental entities in the field of cyberspace protection; 5) representation of the Republic of Poland in international contacts (in the field of military cooperation, in consultation with the Coordination Centre of the Response System to Computer Incidents of the Ministry of National Defence); 5) gathering knowledge about the state of security and threats to the critical ICT infrastructure; 6) responding to ICT security incidents with particular emphasis on the critical ICT infrastructure of the state; 7) representation of the Republic

[9] A.J. Chodubski, *Wstęp do badań politologicznych*, Gdańsk 2004, pp. 125–126.

[10] J. Sztumski, *Wstęp do metod i technik badań społecznych*, Katowice 2005, pp. 183–184.

[11] See K.J. Jakubski, 'Przestępczość komputerowa – zarys problematyki', *Prokuratura i Prawo*, No. 12, 1996.

[12] 'Who we are', *NASK – About us*, https://en.nask.pl/eng/about-us/who-we-are/3261,About-NASK.html [accessed: 10.12.2020].

of Poland in international contacts (in the field of military cooperation, in consultation with the Coordination Centre of the Response System to Computer Incidents of the Ministry of National Defence); 5) gathering knowledge about the state of security and threats to the critical ICT infrastructure; 6) responding to ICT security incidents with particular emphasis on the critical ICT infrastructure of the state.[13]

The reports drawn up by CERT.GOV.PL indicated the need to take actions to protect Polish cyberspace, but also the scale of problems and threats that public administration struggled with in this field. Online incidents and attacks were not uncommon at the time, but various state units were often not interested in reporting such cases to law enforcement agencies. This had a negative impact on the level of security on the Internet and ultimately led to cybercriminals going unpunished.[14]

Numerous problems were also brought to light by the Report on the security of cyberspace of the Republic of Poland in 2011, prepared by CERT.GOV.PL. In 2010, during the scanning of public administration websites, over 1,000 errors were detected, of which 269 could cause a very high level of threat.[15] In 2010, attention was paid to the growing number of dedicated social engineering[16] attacks targeting public administration employees who often exploited their ignorance. Activities of this type included, among others, sending messages with infected attachments.

Table 1. Government cyberspace protection programs developed in 2008–2011

Program name	**Date of creation**
The governmental cyberspace protection program of the Republic of Poland for the years 2008–2011	November 2008
The governmental cyberspace protection program of the Republic of Poland for the years 2009–2011	January 2009
The governmental cyberspace protection program of the Republic of Poland for the years 2009–2011: assumptions	March 2009
The governmental cyberspace protection program of the Republic of Poland for 2011–2015	May 2010
The governmental cyberspace protection program of the Republic of Poland for 2011–2016	June 2010
The governmental cyberspace protection program of the Republic of Poland for 2011–2020	April 2011
The cyberspace security policy of the Republic of Poland	May 2011

Source: authors own study based on: *Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni RP*, https://www.nik.gov.pl/plik/id,8764,vp,10895.pdf [accessed: 10.12.2020].

[13] *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2010 roku*, pp. 3–4, https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/422,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2010-roku.html [accessed: 10.12.2020].

[14] *Ibid.*, p. 5.

[15] *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2011 roku*, pp. 5, 14, https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/422,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2010-roku.html [accessed: 10.12.2020].

[16] Social engineering is the totality of methods and activities aimed at obtaining specific types of behaviour of groups or individuals.

In the report of Poland's Supreme Audit Office (NIK) of 2014, it was emphasised that none of the documents in the table had been approved and accepted for implementation by the Council of Ministers. The reasons given went down to their unreliable preparation and poor quality. The weaknesses concerned a number of issues, such as: lack of deadlines and measures; imprecise goals; failure to identify entities responsible for their implementation; failure to develop draft legislative changes necessary to build a national cyberspace protection system; failure to estimate costs and failure to indicate sources of financing.[17]

In many cases, the problems resulted from different positions at the government level regarding the refinement of the strategy; positions of the Ministry of Finance and representatives of the Chancellery of the Prime Minister, who pointed to the impossibility of transferring additional funds intended for increasing ICT security; legal doubts regarding the form of the document defining the national cyberspace protection strategy, different positions and the competition between the ABW and the Ministry of Interior and Administration management regarding the coordination structure of the cyberspace protection system. The last of the above-mentioned problems was related to staff-related disputes regarding the appointment and filling of the position of the Government Plenipotentiary for Cyber Security of the Republic of Poland.[18]

The 2013 Cyberspace Protection Policy of the Republic of Poland is considered to be the first strategic document on cybersecurity in Poland, which was developed by the Ministry of Administration and Digitisation in cooperation with the Internal Security Agency. The document was adopted by the Council of Ministers in the form of a resolution, and its validity only applied to the government administration.[19] The key goal of the strategy was to achieve an acceptable level of Polish security in cyberspace. Pursuant to this document, government administration units were obliged to assess risk and submit information to the competent minister for computerisation. It was also important to oblige each organizational unit of the government administration to establish an information security management system and to appoint a representative for cyberspace security. As part of the Cyberspace Protection Policy of the Republic of Poland, a three-level National Response System to Computer Incidents was established.[20]

Another document developed at that time was the Cybersecurity Doctrine of the Republic of Poland prepared by the National Security Bureau (BBN) and then approved on 12 January 2015 by the National Security Council (RBN), which was an advisory body to the President of the Republic of Poland. The Cybersecurity Doctrine of the Republic of Poland rests on the assumption that it is a trans-sector executive document to the National Security Strategy of the Republic of Poland, and

---

17 *Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni RP*, p. 34, https://www.nik.gov.pl/plik/id,8764,vp,10895.pdf [accessed: 10.12.2020].

18 *Ibid.*, pp. 32–33.

19 *Polityka Ochrony Cyberprzestrzeni RP*, https://cyberpolicy.nask.pl/polityka-ochrony-cyberprzestrzeni-rp/ [accessed: 10.12.2020].

20 *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*, pp. 6–16, http://jakubow.pl/wp-content/uploads/2015/06/Polityka-Ochrony-Cyberprzestrzeni-RP_148x210_wersja-pl.768174_715482.pdf [accessed: 10.12.2020].

the recommendations of this doctrine are dedicated to be used by all public and private entities involved in activities for cybersecurity. The document postulated taking steps to introduce formal and legal solutions, invest and use the civic potential in the protection of Polish cyberspace[21].

The protection of Polish cyberspace before 2015 required a change of position towards the contemporary challenges related to the protection of this sphere. Numerous problems in many cases resulted from the realization of current political interests, the lack of fundamental knowledge and the awareness of dangers, which at that time were no longer anything new. The characteristics of the threats changed, which required more action. In 2010, there were, inter alia, to attacks on the websites of: the Central Examination Board, the Military Intelligence Service, and the websites of several district courts. As a result of the successful actions of cybercriminals on VoIP Internet telephony, in 2011, a local government unit from the Lubelskie Voivodeship lost PLN 20 thousand, and the local and regional authorities from the Dolnośląskie Voivodeship lost about EUR 40 thousand. CERT.GOV.PL already indicated threats of this type in the previous report from 2010.

Serious financial losses were suffered by the Jaworzno commune, which lost PLN 940 thousand as a result of computer infection by cybercrime.[22] The perpetrators of the attack were students who broke the security of the office's network using a Trojan horse sent electronically. It was not their only theft, 4 other offices were victims of criminals, the total amount was about PLN 2 million.[23] Before 2015, the situation regarding the protection of Polish cyberspace required significant improvement and considerable financial outlays. Building a good system could not take place without the right staff. The NIK report showed that in the controlled period, CERT.GOV.PL employed 12 to 14 people, and the ABW management estimated that 80 to 100 employees were required to properly perform the tasks.[24]

Protection of Polish cyberspace in 2015–2019

During the NATO summit that took place in Warsaw on 8–9 July 2016, a lot of effort was put into looking at issues related to the protection of cyberspace. NATO members, who met in the capital of Poland, adopted over a dozen important documents, including the *Cyber Defence Pledge*. During the summit, the Allies recognised cyberspace as a sphere of operational activities and committed to increasing their defence capabilities in this area. Such a declaration meant that the recognition of a cyber-attack against any NATO member became tantamount to the activation of

[21] *Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej*, Warszawa 2015, pp. 4–5, https://en.bbn.gov.pl/ftp/dok/01/DCB.pdf [accessed: 10.12.2020].

[22] 'Z konta Urzędu Miasta w Jaworznie ukradziono prawie milion złotych', https://www.portalsamorzadowy.pl/prawo-i-finanse/z-konta-urzedu-miasta-w-jaworznie-ukradziono-prawie-milion-zlotych,67083.html [accessed: 10.12.2020].

[23] M. Pietraszewski, 'Studenci hakerzy ukradli z magistratu w Jaworznie prawie 1 mln zł', https://katowice.wyborcza.pl/katowice/1,35063,19007529,studenci-hakerzy-ukradli-z-magistratu-w-jaworznie-prawie-1-mln.html [accessed: 10.12.2020].

[24] *Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni…*, *op. cit.*, p. 40,

Article 5 of the Washington Treaty. The Warsaw NATO summit contributed to the inclusion of defence plans containing cyber threats in the strategic documents of the countries belonging to this organisation.[25]

An important step in improving Poland's security online was the adoption of the Act on the national cybersecurity system of 5 July 2018, which enabled the implementation of solutions provided for in Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016. The adoption of the act on the national cybersecurity system created opportunities for building solutions increasing Poland's security. Despite many criticisms of this legal act, the fact that the act regulates issues related to cybersecurity should be positively assessed. The regulations systematize the organization of the national cybersecurity system as well as the tasks and obligations of the entities that are part of this system. Detailed regulation of this issue made it possible to coordinate activities and indicate the tasks and obligations that were imposed on operators of key services. In line with the adopted solutions, the minister responsible for computerization kept a list of key service operators. The issues related to the Cybersecurity Strategy of the Republic of Poland were also regulated.[26] As many as 270 deputies voted for the bill, 155 were against, and 5 abstained from voting. 29 deputies were absent.[27]

The introduction of the Directive of the European Parliament and of the Council (EU) 2016/1148 of 6 July 2016 on measures for a high common level of security of network and information systems in the territory of the European Union into the Polish legal order forced a number of actions to increase the level of state security in the network. The achievement of the directive's objectives was to be achieved by taking the following actions: 1) establishing a requirement for Member States to adopt a national safety strategy; 2) establishment of network and information security requirements and incident notification; 3) establishing a network of Computer Security Incident Response Teams (CSIRTs); 4) establishing a group whose cooperation will ensure strategic cooperation and exchange of information; 5) establishing obligations relating to the designation by Member States of national authorities, contact points and CSIRTs whose cybersecurity obligations.[28]

Effective action to protect Polish cyberspace required the adoption of a new strategy. By the resolution of the Council of Ministers in May 2017, the National Framework for the Cybersecurity Policy of the Republic of Poland was adopted, which replaced the Cyberspace Protection Policy of the Republic of Poland, in force since 2013. The document was developed by a group of experts from the Ministry of Digitization, Ministry of National Defence, Ministry of Interior and Administration,

---

[25] P. Soloch, P. Pietrzak, 'Szczyt NATO w Warszawie: uwarunkowania, rezultaty, wnioski dla Polski', *Bezpieczeństwo Narodowe*, No. I–IV, 2016, p. 27, https://www.bbn.gov.pl/ftp/dok/03/37-40_KBN_Soloch_Pietrzak.pdf [accessed: 10.12.2020].

[26] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dziennik Ustaw Rzeczypospolitej Polskiej [Journal of Laws of the Republic of Poland] 2018, item 1560.

[27] 'Głosowanie nr 189 na 66. posiedzeniu Sejmu dnia 05.07.2018 r. o godz. 18:21:20', http://www.sejm.gov.pl/sejm8.nsf/agent.xsp?symbol=glosowania&NrKadencji=8&NrPosiedzenia=66&NrGlosowania=189 [accessed: 10.12.2020].

[28] 'ABC cyberbezpieczeństwa na podstawie wymogów dyrektywy NIS', https://rcb.gov.pl/abc-cyberbezpieczenstwa-na-podstawie-wymogow-dyrektywy-nis/ [accessed: 10.12.2020].

Internal Security Agency, RCN, BBN, NASK PIB. The wide spectrum of participants allows the document to be considered interdisciplinary. The involvement of three ministries and several other institutions and organizations changed the perspective of the approach to the issue of state security in the network.[29] The main objective of the document is to ensure a high level of security for the public sector, the private sector and citizens in the field of providing and using digital and key services. Importantly, the National Framework for Cybersecurity Policy emphasizes the need to adopt appropriate legal changes and unify regulations. The authors of the document also saw the need to ensure the safety of entities that manage facilities included in the critical infrastructure.[30]

The general nature of the National Framework for Cybersecurity Policy required experts to develop an Action Plan for the implementation of the National Framework for Cybersecurity Policy of the Republic of Poland for the years 2017–2022. It is a planning document drawn up by members of the Council of Ministers, the Director of the Central Bureau of Investigation and the heads of central offices. Institutions not belonging to the government administration: BBN and NASK also started cooperation in the preparation of the document. The document defines: 1) directions of intervention by government administration bodies until 2022; 2) a list of tasks aimed at achieving the goals of the National Framework for Cybersecurity Policy; 3) a list of activities in relation to the identified tasks; 4) issues of monitoring and reporting. The action plan was adopted in order to systematize the activities necessary to achieve the specific goals of the strategy and the main goal. Another goal for which this document was adopted was to synchronize the approach to the tasks of the involved authorities forming the national cybersecurity system. The authors of the document assumed that the catalogue of tasks and the list of activities would be supplemented every 6 months, and the update would be carried out every 2 years.[31]

In 2017, the then Minister of National Defence Antoni Macierewicz announced the creation of cybernetic troops, the number of which was to be at least 1,000 soldiers within a few years. PLN 2 billion was allocated for this purpose[32]. In September 2019, Mariusz Błaszczak, who at that time was the Minister of National Defence, announced that the command of the Cyberspace Defence Forces would be established by 2022, and their formation would be completed in 2024. Within the Ministry of National Defence (MON), the National Cyberspace Security Centre was established, which is to constitute the core of the cyber defence forces. In order to strengthen the defence potential, a decision was also made to create a component

---

29 'Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022', https://cyberpolicy.nask.pl/rb-dokumenty-krajowe-2-krajowe-ramy-polityki-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2017-2022/ [accessed: 10.12.2020].

30 *Ibid.*

31 *Plan działań na rzecz wdrażania Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022*, pp. 2–3, http://konfederacjalewiatan.pl/legislacja/_files/2017_10/PLAN_KRPC_22-10-2017.pdf [accessed: 10.12.2020].

32 'Macierewicz chce cybernetycznej armii i ma rację. III wojna światowa odbędzie się przez komputer', https://wiadomosci.radiozet.pl/Polska/Macierewicz-chce-wojska-cybernetycznego-i-ma-racje.-III-wojna-swiatowa-odbedzie-sie-przez-komputer [accessed: 10.12.2020].

within the Territorial Defence Forces composed of people who deal with broadly understood IT on a daily basis. As part of the actions taken, the Ministry of National Defence decided to increase recruitment for courses related to cryptology, IT and cybersecurity. On 1 September 2019, the Military General IT Secondary School began operating. In 2024, cyberspace troops are to achieve the ability to conduct operations, which will allow them to be transferred to the command of the General Staff of the Polish Army.[33]

Admittedly, one of the biggest threats on the web is the so-called fake news. False information can disorganise social life, affect election results, and cause panic and chaos. Fighting this phenomenon in the era of social media is a difficult task that requires great awareness of the recipients and constant monitoring and distribution of content that comes from a proven source, guaranteeing their credibility. For this purpose, the Bezpieczwybory.pl portal was established, which is run by NASK. Using this portal, you can report fake news and use the knowledge base. Among the available content there are also reports on this issue.[34]

Between 2015 and 2019, there were many attacks on ICT systems, all over the world, also in Poland. In 2017, institutions from many countries fell victim to the Petya virus, which encrypted computers. The effects of this massive attack were also felt in Poland. The then Prime Minister Beata Szydło, due to the real threat, convened the Government Crisis Management Team. The most spectacular attack in Poland, however, took place at the turn of 2015 and 2016, when the systems of Polish banks and the Polish Financial Supervision Authority (KNF) were hacked. The hackers' activities covered 17 banks and over 200 corporate banks[35]. Phishing attacks aimed at extorting data and money from citizens were increasingly used.

According to the data published in CERT.GOV.PL reports, in 2015–2018, there was an increase in reported incidents. It should be explained here that the sent reports are analysed by the team's analysts. Not every report is tantamount to a security breach. In 2015, CERT.GOV.PL in his report, he indicated 16,123 reports, of which 8,914 were considered actual incidents. In 2016, CERT.GOV.PL recorded 19,954 reports of a potential computer incident, which concerned networks within the team's area of competence. There were 9,288 actual security breaches. In 2017, there were 28,281 reports, of which 5,819 were a security breach. Despite a greater number of notifications in 2017, the number of security incidents decreased. In 2018, there were 31,865 reports, of which 6,236 were a breach of ICT security.

Each of the threats indicated in the table had specific characteristics, which requires a more detailed explanation. A botnet client is a type of malware that runs on workstations connected to the ICT networks of public administration units.[36] Cybercriminals can use computers infected in this way, for example, to send spam or

---

[33] 'Tworzymy wojska obrony cyberprzestrzeni', https://www.gov.pl/web/obrona-narodowa/tworzymy-wojska-obrony-cyberprzestrzeni [accessed: 10.12.2020].

[34] 'Nasza misja', https://bezpiecznewybory.pl/ [accessed: 10.12.2020].

[35] 'Zmasowany atak hakerski na polskie banki', https://www.pb.pl/zmasowany-atak-hakerski-na-polskie-banki-828906 [accessed: 10.12.2020].

[36] *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2015 roku*, https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/910,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2015-roku.html [accessed: 10.12.2020].

carry out attacks. Incorrect configuration of the device is a type of threat that does not have to result from external interference, but allows for an effective attack on the system.[37] A computer virus is software that can replicate itself and is designed to damage a system, for example. Computer infection is often carried out using elements of social engineering. This type of malware can be downloaded, for example, as an e-mail attachment.[38]

Table 2. The most common threats by category in 2016–2018

Year	Type of the most common threat	Amount	Number of all threats
2015	Botnet client	4284	8914
2016	Device configuration incorrect	4158	9288
2017	Virus	1868	5819
2018	Virus	2448	6236

Source: authors own study based on data: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2015 roku*, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2016 roku*, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2017 roku*, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2018 roku*, https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi [accessed: 10.12.2020].

During the rule of Law and Justice in the 2015–2019 term, a number of measures were taken to increase state security in cyberspace. The adoption of the Act on the National Cybersecurity System was an important step that created the formal and legal framework for building a security system. The 2015 NIK report revealed many negligence in the area of cybersecurity. Unfortunately, not all problems could be removed by 2019, as evidenced by the document from the NIK audit; Information security management in local government units. As a result of control activities, it was found that data in local self-governments are poorly protected. The problem is serious and its importance will increase as more and more cases are handled via the Internet. The threat is real, an example of which was the leakage of data from the City of Łódź Office in 2017, concerning garbage declarations, and the leakage of data of some Krakow Card holders in 2018.[39]

As a result of the audit by the Supreme Audit Office, it was found that 16 out of 23 inspected offices did not ensure information security. The problem also concerned the management of user rights in IT systems. In over 80% of the inspected offices there were irregularities in this area, in one of them the employee was blocked from accessing the system during the NIK audit, only 11 years after the appointment. Another reported threat was employee access to an administrator account on official computers, which allowed the installation of any software. The remaining

[37] *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2016 roku*, https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/957,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2016-roku.html [accessed: 10.12.2020].

[38] *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2017 roku*, https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/958,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2017-roku.html [accessed: 10.12.2020].

[39] 'Żeby elektronicznie znaczyło bezpiecznie', https://www.nik.gov.pl/aktualnosci/zeby-elektronicznie-znaczylo-bezpiecznie.html [accessed: 10.12.2020].

problems concerned the non-encryption of data and the use of operating systems without manufacturer support.[40]

Conclusions

Despite the fact that cybersecurity as an issue has grown in importance in recent years, it is necessary to take further actions to increase the level of security. Currently, public administration processes a large amount of data stored in the form of reports and analyses that show the current situation and enable the study of current threats. The functioning of states today is largely dependent on the efficient operation of ICT systems and information security.

The hypothesis outlined in the introduction to this paper has been positively verified. Undoubtedly, cybersecurity in Poland has gained importance for many reasons. At this point, it should be noted that the number of cybercriminals' activities and social awareness in this regard has increased. During the eighth term of the Sejm of the Republic of Poland, the Act on the national cybersecurity system was adopted. However, attention should be paid to the external requirements resulting from membership in NATO and the EU, which in a way stimulated some of the activities aimed at increasing the country's security level in the network. The adoption of a new strategy, which, unlike the document from 2013, was developed by a greater number of entities involved, proves the growing awareness of the threats that arise in this area. The declaration of the creation of troops whose task is to protect cyberspace is a positive impulse but also a great challenge facing Poland. The growing number of matters that can be dealt with by citizens via the Internet is a convenience in everyday life, but also a threat being the object of the growing interest of cybercriminals.

As a result of the study, the answer was obtained to the first research question. During the eighth term of the Polish Sejm, many actions were taken to increase the level of state security in the network. The most important of these are: adopting a new cybersecurity strategy; adoption of the Act on the national cybersecurity system and the implementation of projects aimed at establishing a cyberspace defence force. The answer to the second question requires adding that both NATO and the EU have taken steps to improve security in the area of cyberspace, which concerned all states belonging to these organizations. Due to Poland's membership in the EU, it was necessary to adopt appropriate solutions corresponding to the requirements. It is not possible to provide a full answer to the third question due to the lack of comparable data from 2019. Based on the available information, it can be indicated that the most common threats were computer viruses, incorrect configuration of devices and the threat defined as a botnet client. The large number of phishing attacks also deserves attention.

[40] *Informacje o wynikach kontroli. Zarządzanie bezpieczeństwem informacji w jednostkach samorządu terytorialnego*, pp. 6–19, https://www.nik.gov.pl/plik/id,20027,vp,22647.pdf [accessed: 10.12.2020].

Efforts to increase Poland's security in cyberspace during the 8th term of the Sejm of the Republic of Poland laid the foundations for building a system ensuring security. During the next terms of the Sejm of the Republic of Poland, further activities will be needed to educate people in the field of cybersecurity and educate people. Security is a condition that needs to be built up continuously and cannot be guaranteed once and for all. Some countries around the world in their documents devoted to cyber threats already at the beginning of the 21st century, an example of which is the US, which in 2003 adopted the National Strategy to Secure Cyberspace. During the 9th term of the Polish Sejm, matters relating to cybersecurity continue to play a significant role. At the end of 2019, the Cyber Security Strategy of the Republic of Poland for the years 2019–2024 was published. Building security in the network is a difficult task that requires extensive efforts. Creating effective solutions requires the involvement of many entities, but also citizens who use the network on a daily basis. In many cases, the human being is indeed the weakest link in the entire system.

References

'ABC cyberbezpieczeństwa na podstawie wymogów dyrektywy NIS', https://rcb.gov.pl/abc-cyberbezpieczenstwa-na-podstawie-wymogow-dyrektywy-nis/ [accessed: 10.12.2020].

Bolanowski, J., 'Protest przeciw ACTA, atak hakerów Anonymous, czyli powstanie styczniowe w internecie', https://forsal.pl/artykuly/586784,protest-przeciw-acta-atak-hakerow-anonymous-czyli-powstanie-styczniowe-w-internecie.html[accessed: 10.12.2020].

Chodubski, A.J., *Wstęp do badań politologicznych*, Gdańsk 2004.

Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej, Warszawa 2015, https://en.bbn.gov.pl/ftp/dok/01/DCB.pdf [accessed: 10.12.2020].

'Głosowanie nr 189 na 66. posiedzeniu Sejmu dnia 05.07.2018 r. o godz. 18:21:20', http://www.sejm.gov.pl/sejm8.nsf/agent.xsp?symbol=glosowania&NrKadencji=8&NrPosiedzenia=66&NrGlosowania=189 [accessed: 10.12.2020].

Grzelak, M,, Liedel, K., 'Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu', *Bezpieczeństwo Narodowe* , No. 22, 2012, pp. 125–139.

Informacje o wynikach kontroli. Zarządzanie bezpieczeństwem informacji w jednostkach samorządu terytorialnego, https://www.nik.gov.pl/plik/id,20027,vp,22647.pdf [accessed: 10.12.2020].

Jakubski, K.J., 'Przestępczość komputerowa – zarys problematyki', *Prokuratura i Prawo*, No. 12, 1996, pp. 34–50.

'Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022', https://cyberpolicy.nask.pl/rb-dokumenty-krajowe-2-krajowe-ramy-polityki-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2017-2022/ [accessed: 10.12.2020].

Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022, https://www.gov.pl/attachment/251ae53c-36f7-4eda-8c2c-a4e79d855c08 [accessed: 10.12.2020].

Łapczyński, M., 'Zagrożenie cyberterroryzmem a polska strategia obrony przed tym zjawiskiem', *Komentarz Międzynarodowy Pułaskiego*, No. 7, 2009.

'Macierewicz chce cybernetycznej armii i ma rację. III wojna światowa odbędzie się przez komputer', https://wiadomosci.radiozet.pl/Polska/Macierewicz-chce-wojska-cybernetycznego-i-ma-racje.-III-wojna-swiatowa-odbedzie-sie-przez-komputer [accessed: 10.12.2020].

Marczyk, M., 'Cyberprzestrzeń jako nowy wymiar aktywności człowieka – analiza pojęciowa obszaru', *Przegląd Teleinformatyczny*, Vol. 6, No. 1–2, 2018, pp. 59–72ю

Nasza misja, https://bezpiecznewybory.pl/ [accessed: 10.12.2020].

Pietraszewski, M., 'Studenci hakerzy ukradli z magistratu w Jaworznie prawie 1 mln zł', https://katowice.wyborcza.pl/katowice/1,35063,19007529,studenci-hakerzy-ukradli-z-magistratu-w-jaworznie-prawie-1-mln.html [accessed: 10.12.2020].

Plan działań na rzecz wdrażania Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022, http://konfederacjalewiatan.pl/legislacja/_files/2017_10/PLAN_KRPC_22-10-2017.pdf [accessed: 10.12.2020].

Polityka Ochrony Cyberprzestrzeni RP, https://cyberpolicy.nask.pl/polityka-ochrony-cyberprzestrzeni-rp/ [accessed: 10.12.2020].

Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej, http://jakubow.pl/wp-content/uploads/2015/06/Polityka-Ochrony-Cyberprzestrzeni-RP_148x210_wersja-pl.768174_715482.pdf [accessed: 10.12.2020].

Program Prawa i Sprawiedliwości 2014, http://pis.org.pl/dokumenty?page=2 [accessed: 10.12.2020].

Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2010 roku, https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/422,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2010-roku.html [accessed: 10.12.2020].

Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2011 roku, https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/422,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2010-roku.html [accessed: 10.12.2020].

Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2015 roku, https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/910,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2015-roku.html [accessed: 10.12.2020].

Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2016 roku, https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/957,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2016-roku.html [accessed: 10.12.2020].

Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2017 roku, https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/958,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2017-roku.html [accessed: 10.12.2020].

Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni RP, https://www.nik.gov.pl/plik/id,8764,vp,10895.pdf [accessed: 10.12.2020].

Soloch, P., Pietrzak, P., 'Szczyt NATO w Warszawie: uwarunkowania, rezultaty, wnioski dla Polski', *Bezpieczeństwo Narodowe*, No. I–IV, 2016, https://www.bbn.gov.pl/ftp/dok/03/37-40_KBN_Soloch_Pietrzak.pdf [accessed: 10.12.2020].

Sztumski, J., *Wstęp do metod i technik badań społecznych*, Katowice 2005.

Terlikowski, T., 'Bezpieczeństwo cyberprzestrzeni wyzwaniem naszych czasów. System cyberbezpieczeństwa w Polsce (w świetle obowiązującego prawa)', *Zeszyty Naukowe SGSP*, No. 3 (71), 2019, pp. 75–98.

'Tworzymy wojska obrony cyberprzestrzeni', https://www.gov.pl/web/obrona-narodowa/tworzymy-wojska-obrony-cyberprzestrzeni [accessed: 10.12.2020].
Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dziennik Ustaw Rzeczypospolitej Polskiej [Journal of Laws of the Republic of Poland] 2018, item 1560.
'Who we are', *NASK – About us*, https://en.nask.pl/eng/about-us/who-we-are/3261,About-NASK.html [accessed: 10.12.2020].
Wierzbicki, S., 'Wojny cybernetyczne jako element niekonwencjonalnej konfrontacji międzypaństwowej. Pragmatyczna rzeczywistość, nieunikniona przyszłość', *De Securitate et Defensione*, No. 2(1), 2015, pp. 134–148.
'Z konta Urzędu Miasta w Jaworznie ukradziono prawie milion złotych', https://www.portalsamorzadowy.pl/prawo-i-finanse/z-konta-urzedu-miasta-w-jaworznie-ukradziono-prawie-milion-zlotych,67083.html [accessed: 10.12.2020].
'Zmasowany atak hakerski na polskie banki', https://www.pb.pl/zmasowany-atak-hakerski-na-polskie-banki-828906 [accessed: 10.12.2020].
'Żeby elektronicznie znaczyło bezpiecznie', https://www.nik.gov.pl/aktualnosci/zeby-elektronicznie-znaczylo-bezpiecznie.html [accessed: 10.12.2020].

Działania na rzecz ochrony cyberprzestrzeni Rzeczypospolitej Polskiej w latach 2015–2019
Streszczenie

W artykule podjęto analizę działań dotyczących ochrony polskiej cyberprzestrzeni w latach 2015–2019. Zakreślony w tytule pracy okres dotyczy VIII kadencji Sejmu RP oraz ma ścisły związek z rządami Zjednoczonej Prawicy. Świadomość zagrożeń w cyberprzestrzeni istniała już w latach 80. XX w., co stwarzało podstawy do podejmowania szerszych działań w tym zakresie. Z wielu względów budowa systemu ochrony polskiej cyberprzestrzeni została zapoczątkowana dopiero w XXI w., co istotnie wpłynęło na obecny stan ochrony tej sfery oraz społeczną świadomość istniejących zagrożeń.
Słowa kluczowe: Rzeczpospolita Polska, cyberprzestrzeń, bezpieczeństwo, zagrożenia, Internet

Actions taken to protect the cyberspace of the Republic of Poland in the years 2015–2019
Abstract

The paper looks at the activities related to the protection of Polish cyberspace from 2015 to 2019. The time span referred to in the title concerns the 8th term of the Polish Parliament and is closely related to the rule of the United Right. There had already been a certain level of awareness of the existence of threats in cyberspace back in the 1980s, and this allowed to lay the foundations for wider activities taken in this area. For many reasons, the construction of the Polish cyberspace protection system was only launched in the twenty-first century, which significantly affected the current state of protection of this particular sphere, as well as the public awareness of the threats posed.
Key words: Republic of Poland, cyberspace, security, threats, the Internet

Maßnahmen zum Schutz des Cyberspace der Republik Polen in den Jahren 2015–2019
Zusammenfassung

Der Artikel analysiert die Aktivitäten im Zusammenhang mit dem Schutz des polnischen Cyberspace in den Jahren 2015–2019. Die im Titel des Werkes gekennzeichnete Zeitspanne betrifft die 8. Amtszeit des Sejm der Republik Polen und ist eng mit der Regierung der Vereinigten Rechten verbunden. Das Bewusstsein für die Existenz von Bedrohungen im Cyberspace war bereits in den 1980er Jahren bekannt, was die Grundlage für umfassendere Aktivitäten in diesem Bereich bildete. Aus vielen Gründen wurde der Aufbau des polnischen Cyberspace-Schutzsystems erst im 21. Jahrhundert eingeleitet, was den aktuellen Schutzzustand dieser Sphäre und das soziale Bewusstsein für die bestehenden Bedrohungen maßgeblich beeinflusste.

Schlüsselwörter: Republik Polen, Cyberspace, Sicherheit, Bedrohungen, Internet

Действия по защите киберпространства Республики Польша в 2015–2019 годах
Резюме

В статье проведен анализ действий по защите польского киберпространства в 2015–2019 гг. Отмеченный в названии работы период относится к работе 8-го созыва Сейма Республики Польша и тесно связан с правительством Объединенных правых. Понимание того, что существуют угрозы в киберпространстве присутствовало еще в 80-е годы XX в., и благодаря этому принимались меры по предупреждению киберпреступности. По многим причинам создание системы защиты польского киберпространства началось только в XXI веке, что существенно повлияло на текущее состояние защиты этой сферы и осознание обществом существующих угроз.

Ключевые слова: Польша, киберпространство, безопасность, угрозы, интернет