MODERN MANAGEMENT REVIEW **2022**
MMR, Vol. 27, No. 1(2022), pp 21-32 **January-March**

Witold GRACA[1]

PROTECTION OF CYBERSPACE IN POLAND AND THE CZECH REPUBLIC – THE ROLE OF SECRET SERVICES

Secret services are the key elements in the field of cyber security in Poland. Two of the national CSIRTs (Computer Security Incident Response Teams), i.e. CSIRT GOV and CSIRT MON are run by the following services: the Internal Security Agency and Military Counterintelligence Service. In the Czech Republic, CSIRTs/CERTs at the national level are operated by civilian entities and coordination in the event of a threat is the responsibility of the civilian National Cyber and Information Security Agency (NUKIB). The Polish Act on the National Cyber Security System does not provide for parliamentary control of the activities of national CSIRTs. In the Czech Republic, a special standing committee was established to control the activities of NUKIB. Fundamental differences in the structure of the cyberspace protection system in Poland and the Czech Republic may result from the adoption of different priorities in terms of values by political actors.

Keywords: cyber security, CERT/CSIRT, secret services, Internal Security Agency, Czech National Cyber and Information Security Agency.

1. INTRODUCTION

Back in 1991, the Federal Assembly of Czechoslovakia adopted Act No. 23/1991 introducing the Charter of Fundamental Rights and Freedoms as a kind of common constitution of the federation. This document was created, among others, on the basis of the Universal Declaration of Human Rights (1948), the International Covenant on Economic, Social and Cultural Rights (1966), the European Convention for the Protection of Human Rights and Fundamental Freedoms (1950), and the European Social Charter. The provisions of the Charter are based on the principle of the democratic state of law, which allows the state authorities to interfere with civil liberties only within the limits of the law. After the breakup of the federation, the Charter was adopted by the Czech National Council as the second most valid act after the Constitution of the Czech Republic. "The constitution in the narrower sense of the word and the Charter of Fundamental Rights and Freedoms as a catalog of fundamental rights and freedoms – they form the core of the constitutional order of the Czech Republic" (Vodicka, Cadaba, 2011).

In 1994, when the Czechs were creating their secret services, they very clearly separated the intelligence services from the police services. Czech special services do not have investigative powers. By situating the national cyber security system within the political

[1] Witold Graca, MA, The Institute of Political Science and Public Administration, The University of Opole; e-mail: wgraca@wp.pl. ORCiD: 0000-0002-6226-7750.

system of the republic, Czech politicians placed it outside the secret services in a civilian office established for this purpose and controlled by the parliament.

Within the Polish political system, the processes of developing secret services were different and ultimately led to a continuous increase in their powers. It can be argued that the actors of the Czech political system implement the principles of the democratic state of law or liberal democracy in practice, even with regard to such a sensitive issue in the modern world as the protection of cyberspace. It seems that the model adopted in this respect in Poland goes in a completely different direction.

The aim of the research presented in this article was to compare the systemic and political positioning of cyber security protection in the political systems of Poland and the Czech Republic in the context of the role of secret services, relations between entities performing tasks in this area and the executive and legislative authorities, and the protection of civil rights and freedoms. The analysis used comparative studies "in which at least two cases are examined in at least one aspect" (Karpiński, 2006) and "in which data from more than one culture are compared. [with] data collected in more than one country or state" (Nowak, 2007) as the basic research method and system analysis. The cyber security protection system was treated as a subsystem of the political system of a given country.

2. SECRET SERVICES IN THE CYBER SECURITY SYSTEM IN POLAND – THE INTERNAL SECURITY AGENCY AND THE MILITARY COUNTERINTELLIGENCE SERVICE

In Poland, to manage risk at the national level, implement tasks to counteract cyber threats of a cross-sectional and cross-border nature, handle reported incidents, in accordance with Art. 26 of the Act on the National Cyber Security System (The Act, 2018), which constitutes an implementation of 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 (the so-called NIS Directive), three national Computer Security Incident Response Teams (CSIRTs) have been established: CSIRT MON, CSIRRT NASK, and CSIRT GOV.

CSIRT GOV is run by the Head of the Internal Security Agency (ABW). Leading the CSIRT GOV team is not the only task of the Internal Security Agency in the field of cyber security. The provisions applying to cyber security are those of Art. 5 Paragraph 2a of the Act on the ABW and AW (Foreign Intelligence Agency), which stipulates that the tasks of the Internal Security Agency include

> identification, prevention, and detection of threats to security, significant from the point of view of the continuity of the functioning of the state's ICT systems of public administration bodies or the system of ICT networks covered by the uniform list of objects, installations, devices, and services included in the critical infrastructure, as well as ICT systems of the owners and holders of objects, installations or devices of the critical infrastructure referred to in Art. 5b Paragraph 7 point 1 of the Act of 26 April 2007 on crisis management (Journal of Laws of 2018, Items 1401 and 1560) (The Act on the Internal Security Agency and Foreign Intelligence Agency, 2002).

In turn, via the Act on the National Cyber Security System, Art. 32aa was introduced to the Act on ABW and AW, on the basis of which an early warning system was created in

public administration entities and those included in the critical infrastructure in order to prevent terrorist attacks (The Act on the National Cyber Security System, 2018). This article gives the ABW the right to conduct "security assessments" in the abovementioned entities. They are to be conducted in accordance with a set plan, but also on an ad hoc basis. The manner in which these activities are carried out by the ABW is indicated in Paragraphs 4 and 8 of art. 32a:

> 4. The security assessment consists in carrying out security tests of the ICT system in order to identify vulnerabilities, understood as weaknesses of the resource or security of the ICT system which may be exploited by a threat, affecting the integrity, confidentiality, accountability, and availability of this system (The Act on the ABW and AW, art. 32a paragraph 4.)

Until 2019, CSIRT MON was operated exclusively by the Military Counterintelligence Service (SKW) (The official site of the Ministry of National Defense, 2018). This situation changed in 2020, when, on the basis of Decision No. 58/MON of the Minister of National Defense, Maciej Materka, the Head of the Military Counterintelligence Service, became the new Plenipotentiary of the Minister of National Defense for cyberspace security. The competencies of the new Plenipotentiary included the performance of the tasks referred to in Art. 51 of the Act of 5 July 2018 on the National Cyber Security System, as well as the coordination of cooperation with the National Cyberspace Security Center (NCBC), whose designated sections have been the core of the CSIRT MON and the SKW since 2020. Currently, it is these two institutions from the structures of the Ministry of National Defense (MON), with appropriate expert resources, that jointly carry out tasks in the field of combating threats and ensuring security in cyberspace (The official site of CSIRT MON, 2020).

3. SECRET SERVICES IN THE CYBER SECURITY SYSTEM IN THE CZECH REPUBLIC

The Cyber Security Act in the Czech Republic (Zákon č. 181/2014 Sb., o kybernetické bezpečnosti) was adopted on 29 August 2014 and entered into force on 1 January 2015. In the Czech Republic, completely different legal and organizational solutions have been adopted than in Poland. The Computer Emergency Response Teams (CERTs) listed in the Czech Cyber Security Act, which operate at the national level, were not established on the basis of the structures of special services, but are completely civil structures, which however does not mean that special services are excluded from this system. The national cyber security system in the Czech Republic consists of:

3.1. The governmental CERT unit of the Czech Republic – National Cyber and Information Security Agency (Národní úřad pro kybernetickou a informační bezpečnost – NÚKIB)

Since 2017, the National Cyber and Information Security Agency (Národní úřad pro kybernetickou a informační bezpečnost – NÚKIB) has been responsible for cyber security issues in the Czech Republic. Until 2017, tasks in the field of cyber security were performed by the National Cyber Security Center (Národní centrum kybernetické bezpečnosti – NCKB), which was established pursuant to the Resolution of the Council of Ministers No.

781 of 19 October 2011 (Usnesení vlády č. 781 ze dne 19.10.2011). The Agency (NÚKIB) was established on 1 August 2017 on the basis of Act No. 205/2017 on Cyber Security (Zákon č. 205/2017 Sb.), which amended Act No. 181/2014 (Zákon č. 181/2014 Sb.). NÚKIB is currently the central administrative body for cyber security, including the protection of classified information in IT and ICT systems and in the field of cryptographic protection. NÚKIB constitutes the governmental computer security incident response team (CERT) of the Czech Republic and cooperates with foreign CERTs and CSIRTs as part of its activities.

Meanwhile, the national CERT in the Czech Republic is operated by the CZ.NIC Association. This organization operates under an agreement concluded with the National Cyber and Information Security Agency (NÚKIB). The association is also responsible for leading the national CSIRT.CZ incident response team. The association consists of legal entities that are Internet providers in the Czech Republic. The association has been operating since 1998 and currently has 116 members. The main tasks of the association include keeping a register of Romains registered under the CZ domain, securing the functioning of the CZ domain at the highest level, and conducting training and educational activities (The official site of the Nic.cz Association, Registr domén CZ).

The director of NÚKIB participates in the meetings of the National Security Council (BRS) and is a member of the Cyber Security Committee, which is the BRS's permanent working body for coordinating, planning, and ensuring cyber security of the Czech Republic. Since 2016, the Czech Republic has maintained in its diplomatic representations in the USA and Israel the so-called cyber attaches, diplomats with the rank of counselors, whose task is to establish direct contacts in the field of cyber security with state and private entities in these countries (Zpráva o činnosti Národního bezpečnostního úřadu, 2016).

3.2. Security Information Service (Bezpečnostní informační služba – BIS)

As part of its activities, BIS deals with threats to the security of the Czech Republic's communication infrastructure in the field of cyber security. The tasks of BIS include, for example, investigating various types of electronic attacks aimed at objects of the critical infrastructure, places where classified information is stored, etc. The service collects and analyzes all information regarding real and potential threats and risks related to the use of strategic information in communication systems, the destruction of or the breach in which could seriously affect the security and economic interests of the republic. It concerns computer systems of offices, public administration institutions, and other legal entities that are classified as critical infrastructure. Due to its activities, BIS checks various types of Internet forums where illegal transactions of selling sensitive data take place, or which may serve as contact points or ordering services related to an illegal activity consisting in conducting attacks or obtaining classified information.

The service does not deal with proceedings in the field of industrial security or tasks related to the security of ICT systems (The official site of the Security Information Service, Bezpečnostní informační služba).

3.3. Office for Foreign Relations and Information (Úřad pro zahraniční styky a informace – UZSI)

Czech civil intelligence – the Office for Foreign Relations and Information, which formally functions within the Czech Ministry of the Interior, conducts analytical activities in the field of cyber security.

4. ACTIVITIES WITHIN THE MILITARY SPHERE IN THE FIELD OF CYBER DEFENSE OF THE CZECH REPUBLIC AND POLAND

The Cyber Defense Strategy of the Czech Republic for the years 2018–2022 constitutes a separate document. The difference between cyber defense and cyber security is explained in the introduction to the strategy. According to this stance, ensuring cyber defense should be understood in the context of the comprehensive concept of state defense described in the Act on Ensuring the Defense of the Republic (Zákon o zajišťování obrany České republiky), which regulates all necessary activities aimed at ensuring sovereignty, territorial integrity, the principles of democracy and rule of law, and protection of citizens' lives and property against external aggression (Zákon č. 222/1999 Sb., Zákon o zajišťování obrany České republiky). Contrary to defense, cyber security is understood as a set of measures and activities aimed at protecting the state's cyberspace. These measures may be of legal, organizational, training, or technical nature, etc. The purpose of applying particular measures is to ensure confidentiality, integrity, and availability of information and data in the state's cyberspace.

The strategy is divided into an open and a secret part. The open part presents the basic vision and specific goals, the implementation of which is to significantly increase the defense potential of the republic. The applied measures are, in the assumption of the authors, to take into account the fact that one of the fundamental protected goods is the preservation and defense of fundamental rights and freedoms. The proposed defense measures were designed in line with the principles of proportionality so that the Czech Republic would remain a democratic and safe state (The official site of the Czech Army, Strategie kybernetické obrany ČR).

In accordance with the decision of the government of the Czech Republic of 2015, cyber defense was entrusted to the Military Intelligence (Vojenské zpravodajství). This service is the only Czech military intelligence service within which military intelligence and counterintelligence operate. The National Cybernetic Operations Center (Národní centrum kybernetických operací – NCKO) was established within the structure of this service. Meanwhile, within the Czech armed forces, cyber defense is handled by the Cybernetic Forces and Information Operations Headquarters (Velitelství kybernetických sil a informačních operací). Both of these institutions closely cooperate.

In Poland, the basic document in the field of cyber security which remained in force until 2019, i.e. the National Framework of Cyber Security Policy of the Republic of Poland for the years 2017–2022 for Specific Objective 2 – Strengthening the ability to counteract cyber threats, referred to military activities in cyberspace as follows:

> The Polish Armed Forces, as basic elemenst of the state defense system, must operate in cyberspace as effectively as in the air, on land and at sea. The ability to conduct a full range of military activities in cyberspace must therefore include: identification of threats, protection and defense of ICT systems, and combating sources of threats (https://www.gov.pl, The National Framework of Cyber Security Policy of the Republic of Poland for the years 2017–2022).

In February 2019, a plenipotentiary of the Ministry of National Defense for the establishment of cyberspace defense troops was appointed. Until the establishment of these troops, cyber defense is to be handled by the National Cyberspace Security Center. The unit

was created as a result of the merger of two institutions responsible for ICT security in the army – the National Center for Cryptology and the Information Technology Inspectorate. The tasks of the National Cyberspace Security Center include, inter alia, consolidation of the competencies and resources of the Ministry of National Defense in the field of cryptology (The official site of the Ministry of Digital Affairs). In addition to the abovementioned unit, the Cybernetic Operations Center operated as part of the cyber defense of the Republic of Poland. The Center constitutes a military unit specialized in the full range of military activities and operations in cyberspace. It is the only such unit in the Ministry of National Defense. The Cyberspace Defense Forces are to be formed on the basis of the Center (The official site of the Cybernetic Operations Center, 2018).

5. THE ROLE OF THE PRIME MINISTER IN THE CYBER SECURITY SYSTEM

In the Czech Republic, the highest body coordinating cyber security activities at the governmental level is the National Security Council (Bezpečnostní rada státu – BRS). The Council was established on the basis of Article 9 of Act No. 110/1998 on the Security of the Czech Republic (Ustavní zákon č. 110/1998 Sb., o bezpečnosti České republiky). It is composed of the prime minister and other appointed members of the Council of Ministers. The President of the Czech Republic not only has the right to participate in the meetings of the council, but s/he may also require information from its members and discuss issues that fall within his/her competence.

The Director of the National Cyber and Information Security Agency regularly participates in the meetings of the National Security Council and is a member of the Cyber Security Committee, which is the BRS's permanent working body for coordinating the planning of projects ensuring cyber security of the Czech Republic.

In Poland, the Cyber Security Council operates at the Council of Ministers. It constitutes a consultative and advisory body on cybersecurity matters which is chaired by the Prime Minister. The meetings of the Council are attended, inter alia, by the Head of the Internal Security Agency and the Head of the Military Counterintelligence Service (The Act of 5 July 2018 on the National Cyber Security System, art. 66 paragraph 4).

6. CONTROL OF THE PARLIAMENT

In the Czech Republic, the National Cyber and Information Security Agency (Národní úřad pro kybernetickou a informační bezpečnost – NÚKIB) is subject to the control of the Chamber of Deputies under § 24a of the Cyber Security Act (Zákon o kybernetické bezpečnosti, 2014), which for this purpose appoints a relevant control body in form of a committee. The committee consists of at least 7 members. The Chamber determines the composition of the committee so that every parliamentary club is represented in it. While exercising their mandate, members of the committee have the right to enter the premises of the agency. The deputies are then accompanied by the director of the agency or an employee designated by him/her. The director of the agency submits the following documents to the members of the control body: information on the activities of the agency, draft budget of the agency, evidence necessary to control the implementation of the agency's budget, and internal regulations of the agency. At the request of the committee, the director also provides information on particular security incidents in the field of critical infrastructure, significant information systems, and information systems of key service providers. If the control body

finds that the agency unlawfully restricts or threatens civil rights and freedoms or if the decisions of the agency are defective, the body has the right to demand explanations from the director. The director of the agency is obliged to report to the prime minister any violation of the law, especially in the field of the Cyber Security Act and the Act on Protection of Classified Information, committed by an employee during the performance of his/her duties.

In the Polish Act on the National Cyber Security System, there are no regulations relating to the control of the system by the parliament.

7. DIFFERENCES IN CYBER SECURITY STRATEGY

In 2013, works on a cyber security strategy for the years 2015–2020 began in the Czech Republic. The strategy was accompanied by the Cyber Security Action Plan for the years 2015–2020. The strategy for the years 2015–2020 is not only a vision but also a list of principles that will be followed by the authorities and offices of the republic in the course of attaining their goals. The main principles listed in the document are: protection of fundamental human rights and freedoms and the principles of the democratic state of law, as well as building trust and cooperation between the public and private sectors and civil society. In this context, the strategy states that one of the basic principles of operation of the National Security Agency (the predecessor of the National Cyber and Information Security Agency) in terms of ensuring cyber security is the protection of fundamental rights (https://www.govcert.cz, Národní strategie kybernetické bezpečnosti). In turn, the latest strategy in this area places great emphasis on cooperation with allies, education, and expansion of the expert base (https://nukib.cz, Národní strategie kybernetické bezpečnosti 2020–2025).

In Poland, until 2019, the basic document in the field of cyber security was the National Framework of Cyber Security Policy of the Republic of Poland for the years 2017–2022. This document was adopted by the Resolution of the Council of Ministers of 27 April 2017 and constitutes a kind of strategy. Throughout the text, there are only two passages relating to civil rights and freedoms:

> By taking steps to implement the National Framework of Cyber Security Policy, the Government shall fully respect the right to privacy and take the position that the free and open Internet is an important element of the functioning of the modern society (https://www.gov.pl, The National Framework of Cyber Security of the Republic of Poland for the years 2017–2022)

and furthermore:

> The mechanisms of the information exchange system shall be constructed in such a way as to ensure the protection of the interests of the participating entities, including the protection of business secrets, protection of the image, and protection of other essential values (https://www.gov.pl, The National Framework of Cyber Security of the Republic of Poland for the years 2017–2022).

The National Framework has been replaced by the Cyber Security Strategy of the Republic of Poland for the years 2019–2024. The main goal of this strategy is to increase

the level of resistance to cyber threats and the level of information protection in the public, military, and private sectors, and to promote knowledge and good practices enabling citizens to better protect their information. The latest strategy also states that "government actions will be undertaken with respect for the rights and freedoms of citizens and by building trust between individual market sectors and public administration" (https://www.gov.pl, Cyber Security Strategy of the Republic of Poland for the years 2019–2024).

8. PROTECTION SYSTEMS IN EUROPE

There are different cyberspace protection systems in place in Europe. The most centralized system in this area operates in France. At the same time, France is the only country in the European Union where the development of offensive capabilities enabling the support of military operations has been included in the objectives of cyber security policy. The entity responsible for cyber security policy is the government, and personally the prime minister. Activities in this field are conducted through the General Secretariat for Defense and National Security. The body responsible at the operational level is the National Agency for the Security of Information Systems – ANSSI. The IT Systems Security Operational Center – COSI operates within the structure of the said agency. Meanwhile, CERT operates under the authority of this center. Cyber defense of the entire military sphere is situated within the scope of the Ministry of Defense, and the coordinating body is the specialized Cyber Defense Division (Mickiewicz, 2017).

Great Britain and the Federal Republic of Germany have created rather decentralized cyberspace defense systems. In Great Britain, the central coordinating body is the National Cyber Security Center (NCSC) (CyberDefence24, UK: Inauguracja Narodowego Centrum Cyberbezpieczeństwa). The parent body of the NCSC is the British radio intelligence agency, the Government Communications Headquarters (GCHQ). The executive bodies of the British system are the department of the main ministries. In addition to NCSC, the cyber protection system also includes the Center for the Protection of National Infrastructure (CPNI), responsible for the development of guidelines for managers of objects and elements of the critical infrastructure, and the National Technical Information Office as a coordinator of providing information on the security of critical infrastructure. The units meant to fight specific threats are CERTs (Mickiewicz, 2017).

In the Federal Republic of Germany, there are federal bodies that coordinate and conduct activities in the field of cyberspace protection. The activities in this field are managed by the Federal Government Plenipotentiary for Telecommunications. The function of the forum coordinating cooperation between the administrative and economic spheres is performed by the National Cyber Security Council. The council is composed of representatives of federal ministries: of foreign affairs, internal affairs, national defense, economy, finance, justice and education, the ICT Planning Council, and the delegates of federal state authorities. At the operational level, threats to cyber security are dealt with by the National Center for Counteracting Threats to Cyberspace – NCAZ. The supervision over the center is carried out by the Federal Office for Information Security – BSI (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik, 2009). The NCAZ coordinates the cooperation of federal institutions and federal states in the field of cyberspace protection. At the federal level, these entities include the Federal Office for the Protection of the Constitution (civil counterintelligence – BfV), the task of which is to detect

the initiators of a possible attack, the Federal Office for Civil Protection and Disaster Assistance, Federal Criminal Police Office (BKA), Customs Investigation Bureau, Federal Police, Federal Intelligence Service (BND), and military counterintelligence (Mickiewicz, 2017). The prosecution of the perpetrators of attacks is the responsibility of law enforcement, in particular the police, the BKA, the BfV, and the BSI.

As it seems, the cyber security system in the Czech Republic in the institutional sphere is the closest to the German model. There is one civil office functioning in the system which oversees the entire issue. Secret services are involved in the protection of cyber security, but they perform different tasks in this area, mainly consisting in detecting the perpetrators of hacker attacks or other criminal, espionage, or terrorist events. In the case of the Czech Republic, following the example of German solutions in the process of creating institutions related to security has quite a long tradition. According to Ladislav Pokorny, the first Czech secret service after 1990 was named similarly to the German Office for the Protection of the Constitution (Pokorný, 2012), and furthermore,

> the inspiration derived from the German model of civil counterintelligence (BfV) is visible to some extent in Czech legislation to this day (a narrower concept of the competence of secret services, in the sense of preserving only the informational function, imperative of not concentrating powers, lack of executive powers)" (Pokorný, 2012). One can also add here what Pokorny does not mention, i.e. the enormous emphasis in all planning documents and laws on securing civil rights and freedoms as the basic values of liberal democracy. The very first program of the Civic Forum referred to these values: "the Czechoslovak Republic must be the democratic state of law in the spirit of Czechoslovakian statehood tradition and in the spirit of the applicable international principles, contained primarily in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights (https://www.rozhlas.cz, 1989, Co chce Občanské fórum?, Deset pražských dnů, 17 – 27 listopad 1989, Dokumentace).

It is difficult to compare the Polish cyber security protection system with other systems in Europe. It can only be said that, like in Germany and Great Britain, it is a decentralized system. However, in none of the abovementioned systems do the secret services play such an institutionally dominant role. Only in Great Britain does the coordination body rely on radio intelligence. This may be due to the fact that the development of the Polish security sector went in a completely different direction than that of the Czech Republic. At the very beginning of the transformation in 1989 and 1990, the secret service structures were not separated from the Ministry of the Interior. The services were not deprived of their investigative powers. In later years, only the competencies and powers of the secret services were expanded. Perhaps these processes indicate that in Poland the values of liberal democracy have never taken root in the practice of political life.

9. CONCLUSIONS

1. On the basis of the comparative analysis, it can be concluded that within the political systems of Poland and the Czech Republic, completely different organizational solutions in the field of cyber security have been adopted. In Poland, once again, after granting special services the powers related to the implementation of tasks related to the

protection of classified information, their powers have been extended, this time in the field of cyberspace protection. This task involves the acquisition and processing of tremendous amounts of information in virtually all spheres of life and the interference with civil rights and freedoms. At the same time, the supervisory role in the field of cyber security has been assigned to the executive branch. Polish regulations do not take into account the role of the parliament in controlling the cyber security system.

2. In the Czech Republic, a completely different model from the Polish one was adopted. A civilian central office has been established to protect cyberspace and is controlled by a special parliamentary committee. Cyber security has also been clearly separated from cyber defense dealt with by the military. The protection of human rights and civil liberties is very strongly emphasized in all planning documents of strategic importance. It seems that practically since the establishment of the Czech Republic, there has been a consensus among the Czech political elite not to extend the powers of secret services and other entities in the internal security sector. However, the protection of the principles of the democratic state of law does not lead to chaos in this crucial aspect of state security that is cyber security.
3. The internal security sector is created by the political system and by ruling parties and politicians, but behind them are the values adopted in a given country. The process of building the internal security sector visible in the Czech Republic, consisting in a very clear separation of the activities of secret services from typically investigative activities, the imperative of not concentrating powers and thus also sensitive information and data in a single state institution, which is present in all planning documents, strategies, and laws, as well as the emphasis on the protection of civil rights and freedoms, common to the entire Czech political elite, prove that the values of liberal democracy in the Czech political system are deeply rooted and their observance is obvious. Adopted in Poland as soon as in 1990 by the democratic opposition and continued in the following years, the model, which is different from the Czech one and consists in extending the powers and competencies of secret services, may prove that some other model of democracy is being built in Poland.

REFERENCES

Banasiński, C., ed. (2018). *Cyberbezpieczeństwo. Zarys wykładu*. Warszawa: Wolters Kluwer.

Co chce Občanské fórum?, Deset pražských dnů, 17 - 27 listopad 1989, Dokumentace [access: 13.02.2020]. Access on the internet: https://www.rozhlas.cz/17listopad/dokumenty/_zprava/644374

Cyber Security Strategy of the Republic of Poland for the years 2019–2024 [access: 11.10.2021]. Access on the internet: https://www.gov.pl/web/cyfryzacja/strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2019-2024

CyberDefence24, UK: *Inauguracja Narodowego Centrum Cyberbezpieczeństwa. „Ważna współpraca z sektorem prywatnym"* [access: 12.02.2020]. Access on the internet: https://www.cyberdefence24.pl/uk-inauguracja-narodowego-centrum-cyberbezpieczenstwa-wazna-wspolpraca-z-sektorem-prywatnym

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 [access:14.08.2019]. Access on the internet: https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32016L1148&from=PL

Gesetz über das Bundesamt für Sicherheit in der Informationstechnik [access: 12.02.2020]. Access on the internet: https://www.gesetze-im-internet.de/bsig_2009/

Karpiński, J. (2006). *Wprowadzenie do metodologii nauk społecznych*. Warszawa: Wydawnictwo Wyższej Szkoły Przedsiębiorczości i Zarządzania.

Mickiewicz, P. (2017). *System bezpieczeństwa cybernetycznego państw europejskich. Analiza porównawcza. „Rocznik Bezpieczeństwa Międzynarodowego”,* 2017 [access: 12.02.2020]. Access on the internet: file:///C:/Users/wgraca/Downloads/2017_1_4.pdf

Národní strategie kybernetické bezpečnosti [access: 22.05.2019]. Access on the internet: https://www.govcert.cz/download/gov-cert/container-nodeid-998/nskb-150216-final.pdf

Národní strategie kybernetické bezpečnosti 2020-2025 [access: 11.10.2021]. Access on the internet: https://nukib.cz/download/publikace/strategie_akcni_plany/narodni_strategie_kb_2020-2025_%20cr.pdf

Nowak, S. (2007). *Metodologia badań społecznych*. Warszawa: Wydawnictwo Naukowe PWN.

Pokorný, L. (2012). *Zpravodajské služby*. Praha: Auditorium.

Strategie kybernetické obrany ČR [access: 2.08.2019]. Access on the internet: http://www.acr.army.cz/assets/informacni-servis/zpravodajstvi/strategie-kyberneticke-obrany.pdf

The Act of 24 May 2002 on the Internal Security Agency and Foreign Intelligence Agency (Journal of Laws of 2002 No. 74, item 676) [access: 5.08.2019]. Access on the internet: http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WDU20020740676/U/D20020676Lj.pdf

The Act of 30 August 2011 amending the act on martial law and the powers of the Supreme Commander of the Armed Forces and the rules of his subordination to the constitutional bodies of the Republic of Poland and some other acts (Journal of Laws No. 222, item 1323) [access: 14.08.2019]. Access on the internet: http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20112221323

The Act of 5 July 2018 on the National Cyber Security System (Journal of Laws of 2018, item 1560) [access: 4.08.2019]. Access on the internet: http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WDU20180001560/O/D20181560.pdf

The National Framework of Cyber Security of the Republic of Poland for the years 2017–2022 [access:13.08.2019]. Access on the internet: https://www.gov.pl/documents/31305/0/krajowe_ramy_polityki_cyberbezpieczenstwa_rzeczypospolitej_polskiej_na_lata_2017_-_2022.pdf/0bbc7a32-64df-b45e-b08c-dac59415f109.

The official site of the Czech Military Intelligence [access: 23.05.2019]. Access on the internet: https://www.vzcr.cz/kyberneticka-obrana-46

The official site of the Ministry of Digital Affairs [access: 13.08.2019]. Access on the internet: https://www.gov.pl/web/obrona-narodowa/narodowe-centrum-kryptologii

The official site of the Ministry of National Defense [access: 4.08.2019]. Access on the internet: https://www.cyber.mil.pl/articles/o-nas-f/2018-11-20m-suzba-kontrwywiadu-wojskowego/

The official site of the Nic.cz Association. Registr domén CZ [access: 9.05.2019]. Access on the internet: https://www.nic.cz/page/351/

The official site of the Security Information Service (Bezpečnostní informační služba) [access: 9.05.2019). Access on the internet: https://www.bis.cz/kyberneticka-bezpecnost/

Usnesení vlády č. 781 ze dne 19.10.2011, Ustavení Národního bezpečnostního úřadu gestorem problematiky kybernetické bezpečnosti a národní autoritou pro tuto oblast [access: 9.05.2019]. Access on the internet: https://apps.odok.cz/zvlady/usneseni/-/usn/2011/781.

Ustavní zákon č. 110/1998 Sb., o bezpečnosti České republiky [access: 21.08.2019]. Access on the internet: https://www.zakonyprolidi.cz/cs/1998-110.

Vodicka K., Cadaba L. (2011). *Politický systém České republiky*. Praha: Portal.

Zákon č. 205/2017 Sb., Zákon, kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění zákona č. 104/2017 Sb., a některé další zákony [access: 9.05.2019]. Access on the internet: https://www.zakonyprolidi.cz/cs/2017-205

Zákon o zajišťování obrany České republiky [access: 23.08.2019]. Access on the internet: https://www.zakonyprolidi.cz/cs/1999-222

Zpráva o činnosti Národního bezpečnostního úřadu za rok 2014 [access: 9.05.2019]. Access on the internet: https://www.nbu.cz/cs/informacni-centrum/povinne-zverejnovane-informace/906-vyrocni-zpravy-o-cinnosti-nbu/

Zpráva o činnosti Národního bezpečnostního úřadu za rok 2016 [access: 22.05.2019]. Access on the internet: https://www.nbu.cz/cs/informacni-centrum/povinne-zverejnovane-informace/906-vyrocni-zpravy-o-cinnosti-nbu/

DOI: 10.7862/rz.2022.mmr.02

The text was submitted to the editorial office: November 2021.
The text was accepted for publication: March 2022.