INNOVATIONS IN SECURITY POLICY STEMMING FROM CYBERSECURITY ACT IN THE SLOVAK REPUBLIC IN RELATION TO SELECTED PUBLIC ADMINISTRATION BODIES

[a]GABRIELA DOBROVIČOVÁ, [b]ALENA KRUNKOVÁ, [c]SIMONA FARKAŠOVÁ, [d]ZUZANA HORVÁTHOVÁ

[a]*Pavol Jozef Šafárik University in Košice, Faculty of Law, Gustav Radbruch Institute of Theory of Law, Košice, Slovak republic, gabriela.dobrovicova@upjs.sk*
[b]*Pavol Jozef Šafárik University in Košice, Faculty of Law, Department of Constitutional Law and Administrative Law, Košice, Slovak republic, alena.krunkova@upjs.sk*
[c]*Pavol Jozef Šafárik University in Košice, Faculty of Law, Department of Constitutional Law and Administrative Law, Košice, Slovak republic, simona.farkasova@upjs.sk*
[d]*Metropolitan University Prague, Department of Legal Specialisations and Public Administration, Prague, Czech republic; zuzana.horvathova@mup.cz*

This publication is the result of the research project APVV-17-0561 „Human Rights and Ethical Aspects of Cyber Security“ implemented by the Pavol Jozef Šafárik University in Košice, Faculty of Law.

This publication is the result of the research project No. 68-03 „Public administration, legal disciplines and industrial property“ implemented by the Metropolitan University in Prague and funded by Institutional Support for Long-term Strategic Development of Research Organizations in 2019.

This publication is the result of research project VEGA 1/0720/19 „Innovative strategies in regional policy with a focus on the development of cultural institutions” implemented by the Metropolitan University in Prague.

Abstract: The paper deals with innovations in security policy, which are mainly influenced in relation to cyberspace. Currently, cybersecurity issues are among the most discussed, mainly because most of both the professional as well as personal activities have moved to the online environment. Along the advantages of this phenomenon which undoubtedly include, in particular, the use of the Internet, we may also distinguish in an exponentially increasing magnitude the risks of cyber-hazard of various levels of significance. It is therefore essential to have an institutional framework of public authorities ensuring the safe use of the online environment as well as for dealing with possible security incidents. The aim of the paper is thus to analyze those public administration bodies in the Slovak Republic that have powers in the researched area, as well as to point out the modern trends related to this issue.

Keywords: cyber security, cyberspace, legislation, CSIRT

1 Introduction

Innovation is essential for the successful functioning of the company. Among other things, the transformation of established systems (less functional) into those required by the altered situation is required. Successful functioning of modern public administration depends on a sophisticated organizational system that responds promptly to all of the challenges of social life. Management of public administration in the twenty-first century will not function properly with formerly established procedures and must inevitably reflect new innovations, specifically in the area of information and digitalization of the society. A rapid boom of the so-called cloud services, artificial intelligence and networked IT systems requires both legislative treatment as well as readiness of public authorities for possible negative consequences. At the same time, it is necessary to draw attention to a certain spatial specificity in this area which blurs national borders. Thus, the issue under consideration naturally presupposes the involvement of transnational structures and international organizations. In that vein, the paper aims to analyze the system of public administration bodies that in any way participate in ensuring cybersecurity in the national space of the Slovak Republic. The issue under review is also determined by the fact that the impact of tasks and responsibilities related to ensuring cybersecurity goes beyond the remit of public authorities as it also directly and exponentially affects the private sphere. Therefore, the aim of this paper is to analyze the legislation under the Act on Cyber Security in the Slovak Republic and to point out problematic areas. Using scientific synthesis in the paper enables us to abstract those penetration points that fundamentally change practices and solutions hitherto used in favor of an effective cybersecurity policy. This makes the research area a modern challenge for the scientific community, even in academia. The social government provides not only the fundamental rights, but it is obliged to make positive “social activity” and create a social system focused on the implementation of a social justice (Žofčinová 2015).

2 Cybersecurity policy as one of the key features of public administration bodies in the field of security policy

The subject of security policy is undoubtedly a question of security, the scope of which naturally changes and expands from year to year. Security policy is closely related to defense policy and is in the epicenter of interest of both top representatives of countries as well as of supranational units. (Breichová Lapčáková 2019). From a substantive point of view, security policy could be defined as a set of legislation of a diverse nature, which contains the basic rules for maintaining security or dealing with situations where security is compromised, respectively.

A document forming a basis of the state security policy is usually in the form of a security strategy, reflecting the dynamic development of the security environment, responding to the increasing acuteness, intensity, interconnection and global impact of security threats, as well as the eradication of borders between internal and external security (Majerčák 2016). The security strategy is always based on the values and principles that each state recognizes. The basis for successful implementation of the security policy forms a revised system of public authorities with sufficient competences for potential crisis situations. Thus both the governmental as well as the relevant central state administration bodies have an irreplaceable role in this respect. Current trends consist of the ad hoc establishment of security councils or commissions (Majerčák 2013).

Objective reasons, such as global competition, technological and information revolution, and the development of the security environment create the need to address security threats and challenges through international cooperation. In this sense, an active membership in international organizations, especially the European Union (EU) and the North Atlantic Treaty Organization (NATO), which create some scope for the realization of the common security policy, are of importance for individual states.

In the Czech Republic, the social policy issue is addressed in the social doctrine and is usually understood as a set of legal norms governing social protection including social security assistance, as well as, for example, the protection of women and adolescents in labour relations, as well as other social and legal protection (Chvátalová 2015).

Recently, the security policy has undergone some forms of innovation. The very effect of both computerization as well as the security policy led to the birth of its subgroup, the so called cybersecurity policy. The issue of security policy is complex and requires a wider scope for its analysis. However, due to the purpose of this paper, the authors only focus on its relevance in cyberspace.

The European Union also has a clear position on the subject in the longer term. One of its objectives is to promote the development and dissemination of electronic and information technologies (Articles 179 and 180 of the Treaty on the Functioning of the European Union). However, the implementation of this provision of primary law presupposed the adoption of another series of measures at both the European and national levels.

The Stockholm Programme adopted by the European Council in December 2009 (17024/09) set priorities for the creation of an European area of freedom, security and justice over the next five years. Its content was the result of discussions within the

European Parliament, the Council of the EU, the Member States and the programme stakeholders on the basis of the objectives presented by the European Commission. EU leaders predicted the escalation of cyber challenges in the form of an increasing number of sophisticated threats and attacks presenting a serious threat to the security, stability and economic prosperity of Member States as well as of the private sector and the wider society. At the same time, the importance of keeping the cyberspace open to the free flow of ideas and information and freedom of expression was recognized and thus further regulation took place (Treščáková 2018).

The European Parliament resolution of 12 September 2013 on a cybersecurity strategy of the European Union: an open, safe and secure cyberspace (2013/2606 (RSP)) defines an open, safe and secure cyberspace at the basic level, while laying down a call for all EU Member States to arrange for cyberspace and cybersecurity to constitute one of the strategic pillars of the security and defense policies of each Member State. Looking at the situation in Europe, it is possible to talk about the migration of its inhabitants, particularly towards the New World, over the centuries. The reason for this was the vision of a free and friendly environment in America as such. However, at present there is a significant increase in the immigration to Europe, not because it is poorly populated, but due to the fact that the wealth of Europeans has increased and even the poorer Europeans do not incline to accept any heavy, humiliating or degrading work. In the target countries, therefore, the international migration can be used as a tool to address the specific labour shortage in the labour market (Olejárová Čajka 2016).

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) sets out measures to achieve a high common level of such networks and systems within the EU with the aim to improve the functioning of the internal market. The directive brought along certain obligations for EU Member States, in particular:

- to adopt a national network and information security strategy,
- to set up a network of computer security incident response teams (further as „CSIRT“),
- to promote rapid and effective operational cooperation between Member States and the EU, as well as between individual Member States. This area in EU is covered by ENISA - European Union Network and Information Security Agency.

The developments in this area continue both in practice as well as in law. In September 2018, the Council and the European Parliament opened negotiations, which should have been concluded with the adoption of some common European cybersecurity legislation. Subsequently, Member States responded by adopting the relevant national legislation. At the national level, the Slovak Republic reflected these requirements through multi-level regulation, adopting various strategic and legislative documents.

Moreover, in this sense, the Government of the Slovak Republic created the Cyber Security Concept of Slovakia for 2015-2020, which defined the basis and objectives of the Slovak Republic in the field of cybersecurity. It has defined as the strategic objective in cybersecurity to create an open, secure and protected national cyberspace that would build confidence in the reliability and security of critical information and communication infrastructure, as well as assurance that it will perform its functions and serve national interests in the case of cyber-attacks.

The concept was followed by the "Action Plan for the Implementation of the Cyber Security Concept of Slovakia for 2015-2020", which specifically defined the tasks and the way of their implementation, based on the fact that the Slovak Republic had already taken some steps in that area. The basis of legal regulation creates the Act No. 69/2018 Coll. of 30 January 2018 on cyber security as amended (hereinafter also as "the Cyber Security Act"), which became effective in the Slovak Republic from 1.4.2018.

2.1 Cyberspace

While the social expansion of the computerization offers new qualitative as well as quantitative opportunities, it also brings new, exponentially increasing threats. Cybersecurity policy is thus closely linked to the so-called cyberspace. The notion of cyberspace cannot be ignored even in legal science, although it may still seem to us to be inadequate. It is one of those terms that shall become more internationally established, and only then the countries gradually embrace it in their legal orders. If we want to define it, we must be able to establish its content. Unfortunately, its boundaries are sometimes determined intuitively and the final result often exceeds those boundaries. It is a space based on rules that we do not always understand in whole and, moreover, it changes rapidly within an internal, intangible system. We tend to accept the benefits of cyberspace positively, albeit with caution. We have become accustomed to the global information and communication network, the availability of ad hoc data and information, the speed of data transmission, the use of online platforms, the benefits of which are undeniable. However, sometimes we are unable to identify the risks involved in time and accompanying negative phenomena such as misuse of data (and not only personal data) for unforeseen purposes, or unjustified profit from them. What is worse, those phenomena are usually ahead of any effective regulation. In addition, the connection to the Charter of Fundamental Rights and Freedoms is unmistakable, whether it regards the right to respect for private life and communication, the right to freedom of expression, the right to information, the freedom to conduct business and its protection, or the right to property and privacy policy (Hučková - Rózenfeldová 2018). We must therefore consider that it is important to define at least the basic framework for cyberspace and to regulate the movement of its borders legally.

We may simply define a cyberspace as "an environment composed of worldwide interconnected hardware, software and data networks" (Ottis - Lorents 2010). By specifying it in more detail, cyberspace can also be perceived as "a global space within the information environment the distinctive and unique character of which is limited by the use of electronics and electromagnetic spectrum to create, store, modify, exchange and use information through interdependent and interconnected networks using information and communication Technologies". (Kuel 2009).

According to the Act on Cybersecurity in Slovakia "cyberspace is a global dynamic open network and information system, consisting of activated elements of cyberspace, persons performing activities in this system and relationships and interactions between them" (Article 3, letter b).

These definitions form merely an elementary framework for the purposes of the paper. The authors recognize that the perception of cyberspace may differ in other scientific sectors and at various times. A closely related fact is the emergence of the issue of security or the danger of cyberspace. As regards the notion of cybersecurity, the law refers to a situation in which "networks and information systems are able to withstand to some degree of reliability any action that compromises the availability, authenticity, integrity or confidentiality of the stored, transmitted or processed data or related services provided or accessed via these networks or information systems" (Article 3 letter g).

2.2 Cyberspace security

The Act on Cybersecurity therefore envisages a definition of a certain static phenomenon, the disturbance of which is to some extent permitted via the so called degree of reliability, the scope of which is not specified. It is natural that this term is difficult to define, especially in the electronic sphere, which is the reason why the law maker tried to define it in a negative way and is more concerned with the spectrum of security breaching situations.

As the least dangerous situation it considers the so called *risk* - according to the Act, this corresponds to a degree of cyber threat that is expressed by the probability of the occurrence of an undesirable phenomenon and its consequences (Article 3 letter h). Again, the legislation does not specify the degree of probability is required - whether a minimum indication of the adverse event is sufficient to trigger mechanisms to protect cybersecurity or what is still tolerated as a maximum level where the safety is yet not compromised.

A higher degree of danger is a threat - that is any reasonably recognizable circumstance or event against networks and information systems that may adversely affect cyber security (Article3 letter i).

The Act considers as the most significant breach of cybersecurity the cyber security incident. According to the Act, such an incident may occur either:

1. if any event occurs that has a negative impact on cybersecurity due to a breach of network and information system security or a breach of security policy or binding methodology;
2. if it is a consequence of any event stated below:

- loss of data confidentiality, destruction of data or impairment of system integrity,
- limiting or refusing the availability of a basic service or a digital service,
- high probability of compromising the activities of the basic service or the digital service, or
- threats to information security (Article 3 letter j).

The vagueness and inaccuracy of these terms can be justified in part by the very definition of the scope of the Act, which explicitly states that it only lays down minimum requirements for ensuring cybersecurity (Article 2 (1)). At the same time, it also defines its scope negatively by identifying specific legal relationships which are not covered by its scope such as the requirements for securing networks and information systems under the general regulation on the protection of classified information, the provisions of specific rules on the investigation, detection and prosecution of criminal offenses, the requirements relating to network, infrastructure and information systems security and cybersecurity incidents reporting in the banking, finance or financial system according to special regulations, including the European Central Bank or the European System of Central Banks, etc. (Article 2 (1)).

The definition of the relationship between security and confidentiality plays a role in defining the security boundaries of cyberspace. Under the term “confidentiality” the Act understands a guarantee that the data or information is not divulged by unauthorized entities or processes (Article 3 (d)). We consider confidentiality as one of the most important aspects that make cyberspace a safe space. In the modern age of the Internet, the issue of security is crucial. With the increasing number of technologies, the opportunities to access sensitive data are also increasing. In the Internet space, where private computers, mobile phones, possibly watches, cars or home appliances can be interconnected, a complex network structure arises. This connection of different devices is also commonly referred to as the „Internet of Things”. This very wide branching gives space for little or no control over possible security leaks, which may be an easy mark for experienced cyberspace attackers. Jozef Mintál from Matej Bel University in Café Europa pointed out to one peculiar case from abroad. Some hackers wanted to acquire a lucrative database of gamblers who spent large sums in casinos. Instead of overcoming the complicated protection of the casino computer network, they have chosen an easier route. They managed to get into the thermometer in the aquarium of the casino hall. The thermometer was connected to the internal network, with the help of which they were able to find the database and download it. It was thus confirmed that not only in mechanics but also in cyberspace holds the proverb - the chain is as strong as its weakest link (Mintal, 2018) - its importance. So the question stands, where are the limits of cybersecurity?

3 Institutional framework for cyber security management

The unboundedness of cyberspace requires the interconnection of national and supranational authorities of a similar type. Due to the membership of the Slovak Republic in the European Union, the relevant bodies of the European Union play an essential role in this respect [Hučková – Sokol - Rózenfeldová 2018]. We consider it important to specify that these bodies do not function on the basis of the subordination principle; the EU authorities are rather in the position of coordinating, supporting and advisory bodies towards national authorities.

In the Slovak Republic, pursuant to the Cybersecurity Act, the competences were entrusted to a relatively wide range of competent public authorities. This reflects the fact that the scope of the online platforms is currently so broad that it requires an intervention in almost every area of social life and therefore demands appropriate regulation. According to the Cybersecurity Act, the competence is entrusted to the National Security Authority (hereinafter also the NSA), the Ministry of Transport and Construction of the Slovak Republic, the Ministry of Finance of the SR, Ministry of Economy of the SR, Ministry of Defense, Ministry of Interior, Ministry of Health of the SR, Slovak Information Service, Office of the Deputy Prime Minister for Investments and Informatics and Military Intelligence, which are considered central authorities in the field of cybersecurity (Article 4 letter a). Other ministries and other central state administration bodies within the meaning of the Act No. 575/2001 Coll. on the organization of government activities and the organization of central state administration, as amended (e.g. the Ministry of Justice of the Slovak Republic, the Ministry of Culture of the Slovak Republic, etc.) are entrusted powers in the field of cyber security by the Act, but are not considered as central authorities for cybersecurity (Article 4 letter b). This category also includes the General Prosecutor's Office of the Slovak Republic, the Supreme Audit Office of the Slovak Republic, the Office for Supervision of Health Care, the Office for Personal Data Protection of the Slovak Republic, the Office for Regulation of Network Industries and other state bodies within its competence (e.g. district offices, customs offices, Financial Directorate of the SR, Statistical Office of the SR, etc. (Article 4 letter b).

3.1 National level

The national level of the competent authorities in the Slovak Republic is based on the centralization principle. Since 2016 the National Security Authority has been a central state administration authority for cyber security. In accordance with the legislation in force, it builds technical, personnel and organizational capacities in the field of cybersecurity (e.g. it accredits the CSIRT units – Article 13 of the Cybersecurity Act), solves cybersecurity incidents and builds security awareness in the Slovak Republic. At the same time, the National Security Authority is also a central state administration body for the protection of classified information, encryption service, and cybersecurity and trust services. It is a national contact point for cybersecurity for the European Union, the North Atlantic Treaty Organization (NATO) and the Organization for Security and Cooperation in Europe (OSCE).

Given that cybersecurity is only one of the main powers of the NSA, it established, for the purpose of specialization, the Slovak Computer Emergency Response Team - National Unit SK-CERT. Since 1 September 2019, the NSA transformed that unit into the National Cybersecurity Center SK-CERT - Computer Emergency Response Team (further as SK-CERT). Within the organizational structure of the Authority, the SK-CERT has the status of a separate unit. The national unit SK-CERT is also an accredited member of Trusted Introducer and also a member of FIRST (Forum of Incident Response Security Teams) with a global membership of 490 teams from 92 countries.

SK-CERT primarily provides for:

- national and strategic cybersecurity management and threat analysis activities,
- coordination of dealing with cybersecurity incidents at national level,
- services related to the management of security incidents, the elimination of their consequences and the subsequent recovery of information systems in cooperation with the owners and operators of such systems,
- creation, management and support of cybersecurity competence centers, e.g. tuition, education, training and research.

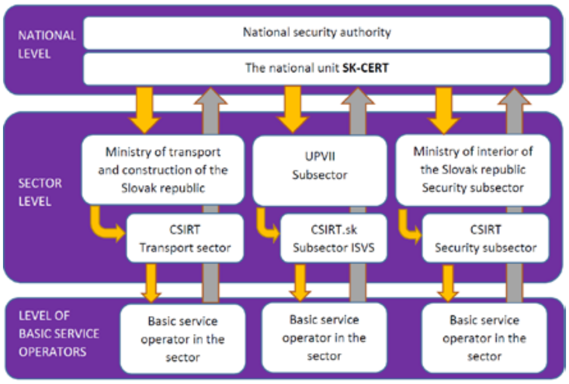
Under the NIS Directive, each Member State is obliged to set up the so-called Computer Security Incident Response Team (hereinafter only as "CSIRT team"). These teams can therefore arise at different levels (national, governmental, academic, armed forces, commercial or other). They differ in the scope of their powers and competences, as well as regards the requirements for their establishment and operation. Such a unit is formed by a team of experts whose main task is to provide the services needed to deal with computer security incidents, mitigate or eliminate their consequences, and subsequently restore the operation of operational information systems and related information and communication means. CSIRT teams differ in terms of groups they aim at. The basis of the social support reform represents the principle of focusing on social assistance, which works on the basis of testing the needs, the essence of which is to direct public funds in areas where it is most lacking. A gradual access to the revision and cancellation of several benefits is essentially connected with introducing the adequate compensation mechanisms for the poor and the most vulnerable. In socially-oriented economies, social assistance takes into account the ethical and moral values of society while respecting human dignity (Žofčinová 2017).

The national unit of CSIRT in the Slovak Republic is the National Cyber Security Center SK-CERT**.** In relation to other CSIRT teams, it has the position of a superior authority, coordinates their activities and creates the basis for strategic decision-making in the area of cybersecurity. Its importance as a national CSIRT unit lies also in the fact that it fulfills the notification and reporting obligations to the relevant bodies of the European Union and the North Atlantic Treaty Organization and also participates and supports the creation of national and international partnerships in the field of cybersecurity. Its powers could be specified in several groups:

- in relation to the national level – it cooperates with central authorities, other government agencies and CSIRT units, basic service operators and digital service providers in the fulfillment of tasks under this Act;
- in relation to users – it receives national reports on cybersecurity incidents, sends early warnings, addresses cybersecurity incidents, alerts and provides warnings regarding serious cybersecurity incident, imposes reactive actions and approves the safeguards, secures and is responsible for coordinated resolutions of cybersecurity incidents that have occurred at the national level;
- in relation to governmental bodies – it systematically acquires, gathers, analyzes and evaluates information on the state of cybersecurity in the Slovak Republic;
- in relation to foreign countries – it receives reports on cybersecurity incidents from abroad and ensures cooperation with international organizations and authorities of other countries in dealing with cross-border cybersecurity incidents and ensures the membership of the Slovak Republic in the cooperation groups as well as in the network of CSIRT units.

In the sense of the NIS Directive, there is the intention of each State to create a sophisticated system of top-down authorities able to respond promptly to any threat of a security incident. Individual central bodies established by the Cybersecurity Act thus have their own CSIRT teams in the Slovak Republic, while under the umbrella of the Deputy Prime Minister for Investment and Information Technology (also UPVII), the CSIRT.SK team also covers the public administration section. This team is a governmental unit in the CSIRT network for the sub-sector of public administration information systems. The CSIRT governmental unit must meet the conditions of accreditation under Art. 14 and must also fulfill the tasks under Art. 15 of the Cybersecurity Act. The CSIRT government unit is also included in the list of accredited CSIRT units maintained by the NSA.

Fig. 1: Outline of organizational structure


NATIONAL LEVEL
National security authority
The national unit SK-CERT
SECTOR LEVEL
Ministry of transport and construction of the Slovak republic
UPVII Subsector
Ministry of interior of the Slovak republic Security subsector
CSIRT Transport sector
CSIRT.sk Subsector ISVS
CSIRT Security subsector
LEVEL OF BASIC SERVICE OPERATORS
Basic service operator in the sector
Basic service operator in the sector
Basic service operator in the sector

Source: Cyber Security Association Workshop (July 9, 2019)

CSIRT units' tasks are of a substantial nature and play an important role in cybersecurity, as their prompt response can often avert disaster. In terms of their activities, these can be classified as reactive services (e.g. incident resolution, incident detection, warnings and alerts, providing on-site incident resolution, proposing measures to prevent the continuation, spread and reoccurrence of incidents, malware analysis, etc.) and as proactive services. As regards the latter, these include services such as education (Tirpák 2011) and awareness building in the field of information security, vocational training and cooperation, cooperation with other CSIRT units, consulting activities in the field of information security, information security audit or assistance in setting up new CSIRT units, which play an essential role in the creation of the so-called bottom-up safety.

This relates to the fact that CSIRT teams created by commercial companies and universities dominate in the world, whereas in the Slovak Republic their gradual integration in the position of public administration takes place. However, given the fact that most of the work as well as personal activities are already carried out in the online environment, we are in a situation where it is necessary to ensure the environment of non-professional community by competent authorities that will foster the cybersecurity.

The report prepared by CSIRT.SK team in August 2019 (CSIRT.SK, 2019) shows that the protection of the state is inadequate in cyberspace, and therefore the Slovak Republic has to embark on the path of enlightenment for ensuring the security in cyberspace. On the basis of the above stated, it is gratifying that there is at least an essential involvement of the non-professional feature, which is the Slovak Security Policy Institute, operating the Slovak cyber security portal CyberSec.sk, which has since 2014 served as a central platform for the Slovak cyber security community.

At the same time, the Association of Cyber Security acts as a voluntary and independent civil association, the aim of which is to represent the Slovak information and cybersecurity community in the role of its professional organization.

3.2 Open Co-operation

The position and nature of cybersecurity policy implies that the success of its security often depends on a network of mutual cooperation that is constantly evolving and developing. For the purposes of this paper, we refer mainly to the following links related to the active portfolio of European cooperation.

In the area of the European Union organizationally operates, for example, the ENISA - the European Union Agency for Cybersecurity (sometimes referred to also as the European Network and Information Security Agency), which is a very center of cybersecurity expertise in Europe. It is a partner of government CSIRT units of individual Member States. Headquartered in Heraklion, Crete, its operations office is located in Athens. Since its establishment in 2004, ENISA has been actively contributing to a high level of network and information security in the Union, raising awareness of network and information security in society and developing a culture in this field.

An important role in this respect is also played by the European Cyber Security Organization (ECSO), which has, since 2016, brought together more than 200 public authorities, private sector entities as well as academia from 27 countries. Its main objective is to support all kinds of initiatives or projects aimed at developing, promoting and fostering European cybersecurity, promoting and protecting the European digital single market from cyber threats, and developing and increasing the competitiveness of the ICT sector (further as ICT). It is a rare combination of public-private partnerships that benefit from sharing innovative practices and solutions for different sectors.

The Central European Cyber Security Platform (CECSP) was established in 2013 at the initiative of both the Czech Republic and Austria. It consists of representatives of government, national and military CSIRT teams, together with national security authorities and national cybersecurity centers from Slovakia, the Czech Republic, Poland, Hungary and Austria. The aim of the platform is an intensive cooperation of neighboring countries in the field of cybersecurity, in particular the exchange of information and sharing of know-how on cyber threats, as well as on potential and already performed cyber-attacks.

The Organization for Security and Co-operation in Europe (OSCE), which since 1995 brings together up to 57 countries in Europe, Central Asia and North America, has also strengthened its prominent position. For cybersecurity issues, it has a Security Committee in the format of the Informal Working Group (IWG) for dealing with cyber issues.

At the same time, the competent authorities of the Slovak Republic cooperate with partner governmental authorities, especially of neighboring countries (e.g. with the Czech National Cyber and Information Security Agency), or of those Member States that intensify proactive cooperation themselves (e.g. the French ANSSI - Agence Nationale De La Sécurité Des Systèmes D'information, or GOVCERT.LU of the Grand Duchy of Luxembourg), respectively.

4 Conclusion

Cybersecurity is one of the areas developing at maximum speed. At present, the lex generalis in terms of public administration embodies the analyzed Cybersecurity Act as well as the act No. 95/2019 Coll. on Information Technologies in Public Administration as amended. Along with the implementation of the general intention of computerization, which is the gradual centralization of public administration information systems and their operation in the cloud environment, it is necessary to create a process for the gradual centralization of cybersecurity management, which is currently in the development phase.

According to the document Strategic Priorities: Information and Cybersecurity prepared by the Office of the Deputy Prime Minister for Innovation and Information Technology and approved on July 25, 2019, it follows that the SR does not have sufficient professional capacities to solve the necessary tasks at central and departmental level, or necessary experts to ensure the protection of its own systems. However, neither the private nor the academic sectors have the necessary experts (in number and focus) and the security of the state cannot be based on external collaborators.

However, for the effective cybersecurity coordination process it is essential that an effective way of enforcing security measures in public administration is established. The aim of the National Cyber Security Center SK-CERT will thus be not only to develop capabilities to deal with cybersecurity incidents at national level, but also to expand and share knowledge and experience in this area and to actively cooperate with the public, professional organizations and the academic sector.

A joint effort to innovate cybersecurity measures strengthens the positions of stakeholders in the international environment. In order to ensure cybersecurity, it is necessary to find a consensus on addressing new security challenges and to jointly promote that consensus at a pan - European scale. In May 2019, the Council of the European Union introduced a sanctions regime that allows the EU to take targeted restrictive measures aimed at discouraging and combating cyber-attacks posing an external threat to the EU and its Member States. The new sanctions regime is part of the of EU Cyber Diplomacy Toolbox, which is a framework for a common EU diplomatic response to harmful cyber activities, allowing the EU to take full advantage of the Common Foreign and Security Policy measures. These include e.g. statements by the High Representative, diplomatic demarches and, where necessary, restrictive measures to respond to harmful cyber activities.

Finally, it should be added that the security policy as a whole is also closely influenced by the government and the political situation in the country. Its stability is undoubtedly improved with the stability of the executive power in the state, which guarantees the continuity of change and innovation. The Slovak Republic’s recent parliamentary elections and its outcome will definitely affect the future direction of cyber security within the security policy.

Literature:

1. ABRHÁM, J. (2011). *Ekonomická, sociální a územní diferenciace Evropské Unie*. 1. ed. Praha: Vydavatelství MAC, 2011. 147 p. ISBN 978-80-86783-52-9.
2. BREICHOVÁ LAPČÁKOVÁ, M. (2019) Univerzálne ius cogens a ústavné limity výkonu verejnej moci v judikatúre Ústavného súdu Slovenskej republiky. In: *Ústavné dni : tretie funkčné obdobie Ústavného súdu Slovenskej republiky - 7. ústavné dni.* Košice: Kancelária Ústavného súdu Slovenskej republiky 188-204 p. ISBN 9788081291029.
3. ČAJKA, P.: *Present Demographic Problems*. In: Dufoulon, S. & Rošteková, M.: Migrations, Mobilités, Frontières & Voisinages. Paris: L`Harmattan, 2011, 115-124 p. ISBN 978-2-296-56363-6.
4. HUČKOVÁ, R. - SOKOL, P. – RÓZENFELDOVÁ, L. (2018) 4th industrial revolution and challenges for European law (with special attention to the concept of digital single market). In: *EU and comparative law issues and challenges series: Eu law in context – adjustment to membership and challenges of the enlargement.* International Scientific Conference. - Osijek: Sveučilište Josipa Jurja Strossmayerau Osijeku, 2018. 201-215 p. ISBN 9789538109249.
DOI: https://doi.org/10.25234/eclic/7107. Available at: https://hrcak.srce.hr/ojs/index.php/eclic/issue/view/313/Vol2.
5. HUČKOVÁ, R. - RÓZENFELDOVÁ, L. (2018) Ochrana súkromia na internete. In: *Bratislavské právnické fórum* 2018: *ústava na internete a internet v ústave*. - Bratislava: Právnická fakulta, 2018. 57-66 p. ISBN 9788071604822.

6. CHVÁTALOVÁ, I. (2015). Veřejnoprávní základy sociálního zabezpečení v České republice a Evropské unii. In: Klíma, K. a kol. *Veřejná správa a lidská práva*. Praha: Metropolitan University Prague Press. 183 p. ISBN 9788087956274.
7. KUEL, D.T. (2009) From cyberspace to cyberpower: Defining the problem. Cyberpower and national security, 2009. 24 – 42 p. ISBN 9781910810835.
DOI: https://doi.org/10.2307/j.ctt1djmhj1.7
8. MAJERČÁK, T. (2013). Creation power of the president of the Slovak republic. In: *Przeglad Prawa Konstytucyjnego* No.1(13), 111-142 p. ISSN 2082-1212.
DOI Address: https://doi.org/10.15804/ppk.2013.01.06
9. MAJERČÁK, T. – GRABOWSKA, S. (2016) Zasady podzialu wladzy na Slowacji. In: *Zasady podzialu wladzy we wspolczesnych państwach europejskich.* Tom2. - Rzeszów : Wydawnistwo Uniwersytetu Rzeszowskiego 110-128 p. ISBN 9788379963706.
10. OTTIS, R. – LORENTS, P. (2010) Cyberspase: Definition and implications. In: *International Conference on Information Warfarw and Security*. Academic Conferences International Limited, 2010. 267 p. ISBN 9781908272553.
11. OLEJÁROVÁ, B., ČAJKA, P. (2016). Third countries migration and the immigrant investor programs in the EU - the case of Chinese immigrants in Portugal. In: *ICEI 2016: proceedings of the 3rd international conference on European integration 2016*. Ostrava: VŠB Ekonomická fakulta. 689 - 697 p. ISSN 2511-2252
12. SVOBODOVÁ, M. (2016). Ochrana proti nečinnosti orgánů Evropské unie. *Právní rozhledy* č. 7/2016, 242-248 p. ISSN 1210-6410.
13. SVOBODOVÁ, M. (2016). Kolize závazků plynoucích z unijního práva a mezinárodního práva. *AUC-Iuridica* č. 2/2016, 127-140 p. ISSN: 0323-0619.
14. TIRPÁK, P. (2011) Výchovné prostredie a jeho vplyv na medzigeneračný dialóg v rodine. In: *Kvalita života a ľudské práva*. Prešov, 2011 151-161 p. ISBN 9788055503431.
15. TREŠČÁKOVÁ, D. (2018) On some aspects of protection of personal data in the European area. In: *Topical issues problems of modern law and economics in Europe and Asia*. Moskva: Moskovskij gosudarstvennyj juridičeskij universitet imeni O. E. Kutafina, 2018. 144-162 p. ISBN 9785720514969.
16. UŠIAK, J. 2011 European Political Culture and European Community. In *Identités, citoyennetés et démocratie: 20 ans aprés = Identities, citizenship and democracy: 20 years after.* Bruxelles: BRUYLANT, 2011. ISBN 978-2-8027-3085-9, 109-121 p.
17. ŽOFČINOVÁ, V. (2015). Social Rights and Dignified Work in Labour Law Relations. In: *Ius et Administratio*. 58 - 68 p. ISSN 2300-4797. Available at: http://iusetadministratio.eu/32015-586.html [Access: 2017-07-12].
18. ŽOFČINOVÁ, V. (2017). Factors influencing the provision of social welfare services at the level of territorial self-government of the Slovak Republic. In: *Administratie si Management Public*. (29). 27 - 40 p. ISSN 1583-9583.
19. MINTAL, J. Available at: https://w.soundcloud.com/player/?url=https%3A//api.soundcloud.com/tracks/603893016&auto_play=false&hide_related=false&show_comments=true&show_user=true&show_reposts=false&visual=true.
20. Strategic priority: Information and cyber security. Office of the Deputy Prime Minister of the Slovak Republic for Investments and Informatization. Bratislava. 25.7.2019
https://www.vicepremier.gov.sk/wp-content/uploads/2019/08/SP_Inform_kybern_bezpecnost_schvalena_2019_07_25_v1.0.pdf
21. The Stockholm Programme of the European Council of 10 and 11 December 2009 n. 17024/09.
22. Monthly report CSIRT.SK (August, 2019). https://www.csirt.gov.sk/aktualne-7d7.html?id=202

Primary Paper Section: A

Secondary Paper Section: AG