Acta Univ. Sapientiae, European and Regional Studies, **19** (2021) 72–87

DOI: 10.2478/auseur-2021-0005

Cyber Security Strategies of the Visegrád Group States and Romania[1]

Milada NAGY
PhD, Budapest Business School University of Applied Sciences, Budapest
Faculty of International Management and Business
Department of International Relations
e-mail: nagy.milada@uni-bge.hu

Abstract. Among security challenges that have emerged on nation-state level, attacks in cyber space are 'products' of the recent past. Their significance has been overvalued especially in 2007 owing to the cyber attack against Estonia. As a consequence, it were not only the European Union (EU) and the North-Atlantic Treaty Organization (NATO) to have created their own cyber security strategies but the majority of states have also made preparations for preventing and deterring threats from the cyber space. States of the Visegrád Four (V4) and Romania, though all full members of both the EU and the NATO, have prepared their own cyber security strategies.

The objective of this study is to offer a comparative analysis of cyber security strategies of the Czech Republic, Poland, Hungary, Slovakia, and Romania, contrasting them to the relevant documents of the EU and the NATO, pointing out the identities and differences. A further essential element of the research is the description of the cooperation between V4 members in the implementation of cyber security strategies and of the chances of broader regional cooperation in the given field based on the jointly adopted documents or on other grounds. One important step in this area was the adoption of the Central European Cyber Security Platform in 2013. This common move, joined also by Austria, is directed mainly at technical exercises. However, the functioning of the Platform is not free from difficulties. Therefore, V4 members have undertaken to find common solutions, including education and professional training for the further development of regional cooperation and widening its spectrum.

Keywords: Visegrád Four, Poland, Romania, Hungary, cyber security, strategy

1 This paper was presented at the conference *Past, Present and Future of Central Europe*, organized by Budapest Business School and Sapientia Hungarian University of Transylvania in Cluj-Napoca on 20 November 2020 (online conference).

Introduction

It is not exclusively our life that is made easier and more efficient by information and communication technologies but also public administration. The world relies more and more on information technology (IT) methods; therefore, the trends of threats are continuously changing, and nowadays the state-financed, well-organized attacks are typical. Even at the World Economic Forum in 2013, it was stressed that among the global challenges the size of the economic and physical damage caused by terrorism had been exceeded by that related to cyber-attacks (WEF 2013).

The well-known cyber-attacks (in 2007 against Estonia, the war between Russia and Georgia in 2008, the Stuxnet attack against Iranian nuclear facilities in 2010) inspired the states to create their own cyber security strategies and develop the defence of their IT systems to the highest level.

The article analyses the cyber security strategies of the Visegrád Group countries (the Czech Republic, Hungary, the Republic of Poland, and the Slovak Republic) and Romania. Its main aim is to support the oversight of existing strategies by the utilization of its conclusions and the correction of drawbacks and to give help for those countries that are yet to draw up their own documents.

Background

Before starting the analysis of the cyber security strategies of the Visegrád Group and Romania, it is important to clarify the changes in the meaning of strategy as a term, furthermore the interpretation of cyberspace and cyber security. The term 'strategy' goes back to the Greek word *stratēgos* and means 'main military leader'. In the past, it was the planning of military operations and troop movements that was described by the word 'strategy'. Over time, the meaning underwent some transformation. In our days, it means 'the complex application of opportunities' states have in the international arena as a result of the aforementioned transformation (Csiki 2008).

The concepts of cyberspace and cyber security have been defined by several researchers. The author applies in both cases the definitions of László Kovács, a Hungarian cyber security expert. Cyberspace is:

> an umbrella term applied to users, instruments, software, processes, information stored or under transmission, services, and systems that are directly or indirectly connected to computer networks (...) Cyber security is a complex of security-determined instruments, policies, conceptions, technologies, perceptions, risk management methods, activities, trainings, the whole of best practices, whose aim is to protect the computer environment

used by organizations and users and to protect their devices and systems (Kovács 2018: 18).[2]

It is the constitution or basic law that is at the top of the system of strategic documents encompassing the national values and interests whose defence is a state priority. It follows that this endeavour is bound to appear in the highest-level strategic document, namely in the national security strategy. Besides the formulation of objectives, the environment is usually also defined, wherein the state wishes to achieve its goals. The challenges that exist at the time of drawing up this document as well as their evaluation also form part of the document.

The proposals and guidelines of the North Atlantic Treaty Organization (NATO), the specialized telecommunications organization of the United Nations, namely the International Telecommunication Union (ITU),[3] and in the European Union those of the European Union Agency for Network and Information Security (ENISA)[4] are decisive. Regarding the ENISA proposals, the most important step is to define the goals. The ENISA assigns several tasks to it:

1. Define the vision and scope that set the high-level objectives to be accomplished in a specific time frame (usually 5–10 years).

2. Define the business sectors and services in scope for this strategy.

3. Prioritise objectives in terms of impact to the society, economy and citizens (see Chapter 4 for examples of potential objectives).

4. Define a roadmap for the implementation of the strategy, which may involve the following steps.

5. Define concrete activities that would meet the objectives of the strategy.

6. Develop a governance framework for the implementation, evaluation and maintenance of the strategy.

7. Develop a master plan for the implementation of the strategy.

8. Develop concrete action plans for each activity.

9. Define the evaluation of the strategy and its main actions (e.g. which key performance indicators (KPIs) will be performed and by whom. (ENISA 2016: 14)

2 The quotation was translated by the author.

3 The International Telecommunication Union is an organization with 193 member states – moreover, several companies, universities, international and regional organizations have joined it. Its main goal is the international harmonization of infocommunication technology and telecommunication. The three central topics are radiocommunication, the international standardization and harmonization of telecommunication, and the international development in the infocommunication sector (ITU 2020).

4 The European Union Agency for Network and Information Security founded in 2004 is one of the cybersecurity organizations of the European Union. The headquarters is in Heraklion (Crete, Greece). The agency plays an active role in the formulation of cybersecurity strategies of the EU Member States by giving advice, supporting governments with experience, and providing consultation opportunities.

The ENISA proposal highlights the importance of involving the private sector NGOs in the strategy-making process. The reason why civilians are important is that citizens' awareness is a pivotal issue. Individuals are listed as the most important actors in cyberspace because Europe has an Internet penetration of about 80%. (*Table 1* shows data related to the five countries analysed.)

Table 1. *Internet users in the world (2020). The number of Internet users was 4.93 billion worldwide (63.2% of the world population)*

	Internet Users	Total Population (2020)	Non-Users (Internetless) (%)	1 Year User Change (%)	Population change (%) between 2019 and 2020
Czech Republic	85	10,693,939	9	1	0.7
Hungary	85	9,769,526	9	5	-4.0
Poland	78	37,958,138	15	4	-3.1
Romania	72	19,328,838	18	4	-7.4
Slovakia	82	5,4579,873	12	4	0.3

Source: data of DESI 2020, EUROSTAT 2021

Table 2 shows the ranking of the countries analysed by Global Cybersecurity Index (GCI).[5] Poland's 29th and Hungary's 31st positions in the world should be given a positive evaluation.

Table 2. *Ranking of the countries analysed by Global Cybersecurity Index 2020*

	GCI European ranking	GCI global ranking
Czech Republic	35	68
Hungary	22	35
Poland	18	30
Romania	32	62
Slovakia	21	34

Source: GCI 2021

Analysis of the Strategies

The basis of the research is formed by the documents[6] of the countries analysed, published in English and downloaded from the European Union Agency for Cybersecurity (ENISA) homepage, and by the following aspects:

1. time when the document entered into effect (in the case of several versions, we focus on the latest document),

5 The Global Cybersecurity Index considers 25 various viewpoints during the evaluation. These include, among other things, the existence of strategy and the willingness to update it regularly.

6 The homepage of ENISA metions the new version of the Hungarian government in 2018, but only the version of 2013 can be downloaded.

2. strategic objectives,
3. clarification of key terms (e.g. cyberspace, cyber security, etc.),
4. perception of cyber threats,
5. cyber security organizations at the national level,
6. listing of critical infrastructure[7] and sectors,
7. existence of incident response capabilities,
8. measures (e.g. regular overview of documents), and
9. cooperation between the international and national governmental and non-governmental actors.

The Republic of Poland

The cybersecurity strategy[8] of the Republic of Poland adopted in 2017 is a new version of the one from 2013 and is valid for a five-year period. Its subtitle underlines that cybersecurity is an important part of state policy (NCSS-PO 2017). The strategy envisages as its main goal the provision of safe electronic services for the population, the public and private sectors. Four specific objectives are described: (1) to increase 'capacity for nationally coordinated actions', (2) to enhance 'capacity to counteract cyberthreats', (3) to increase 'the national potential and competence in the area of security in cyberspace', and (4) to build 'a strong international position of the Republic of Poland in the area of cybersecurity' (NCSS-PO 2017: 7). The objectives mentioned are described in detail in chapters 5–8.

The statutory environment is raised to the ministerial level. The Minister of Digital Affairs is responsible for cooperating with other ministries for undertaking legislative work in order to regulate specialized tools developed for the field of military operations in cyberspace as well as for monitoring and updating the regulation (NCSS-PO 2017: 9).

The lack of sufficient cooperation (between civilian and military actors, public and private sectors) is blamed for the reduced efficiency of the system. This problem has been emphasized by the strategy, wherefore it should be remedied by setting up the National Cybersecurity Centre, the national and sectorial incident response

7 Pursuant to the Hungarian law No. CLXVI. of 2012, the critical infrastructure is 'part of an instrument, facility, or system belonging to certain sectors, which is necessary for the completion of essential social tasks – especially for healthcare, the personal and property security of the population, the providing of economic and social public services –, and services whose stoppage […] would cause significant consequences' (CLXVI. 2012).

8 Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022. Poszanowanie praw I wolności w cyberprzestrzeni, kompleksowe podejście do bezpieczeństwa, cyberbezpieczeństwo istotnym elementem polityki państwa (National Framework of Cybersecurity policy of the Republic of Poland for 2017–2022. Respecting the rights and freedoms in cyberspace, comprehensive approach to security, and cybersecurity as an important element of the state policy).

teams (CSIRTs), and the information exchange and analysis centres, furthermore by the extension of CSIRT networks to the national, sectorial, commercial, and corporate levels in the near future. As far as international cooperation is concerned, it is the European Union, the North Atlantic Treaty Organization, and the Visegrád Group that are mentioned in the first place; additionally, other international actors, among them, governmental and non-governmental organizations.

The strategy highlights the importance of delineating those operators that are responsible for the indispensable services or critical infrastructures. Parallel to this, the security of information and communication technology (ICT) will be developed. The government has undertaken to create new regulations for the digital service providers and for the 'digital single market' in Poland (NCSS-PO 2017: 12).

In the field of secure ICT systems, it is absolutely necessary to have access to information; therefore, Poland is going to establish a system at the national level. Its main task will be to warn and inform – bearing in mind the security of sensitive information and data. An additional system will protect the population as end users 'from the effects of identified threats' (NCSS-PO 2017: 14).

The preparation for the prevention and protection of threats that are growing in number needs state support, chiefly in the field of action coordination and fight against crimes. The efficient, fast, and reliable exchange of information between states, organizations, and service providers is indispensable in threat detection.

In the area of military operations, the Polish Armed Forces should dispose of the full range of capabilities, including threat recognition, thwarting of threats at the source, and the protection of information systems.

The National Cybersecurity Centre will help to increase Poland's cybersecurity by analysing internal and external information. A further important goal is to develop the technology and the industry and to support research. By the creation of the Cyberpark Enigma Program, high-quality hardware and software can be produced and people can be made knowledgeable – all these are part of cybersecurity. As a result, Polish companies can become competitive in the European Union in the field of ICT services. The Polish government is also planning to expand the cybersecurity competence of research institutions as well as to set up the Scientific Cybersecurity Cluster with a view to raising awareness in the circle of individuals and professionals by way of education activities.

The strategy includes a promise to create a Cybersecurity Action Plan six months after its coming into force. Ideally, the Action Plan will be financed by the national treasury, the National Centre for Research and Development, and the European Union.

The area-specific terms applied in the ten chapters of the strategy are explained in Chapter 11.

The Czech Republic

The cybersecurity strategy of the Czech Republic – the new version of the original from 2011 – came into force in 2015 and was prepared for a five-year period (NCSS-CZ 2015). The nine chapters list the perspectives, the principles, the challenges, and the main goals of the state and also their feasibility in the area of cybersecurity. Regarding the Czech strategy, the main aims are: (1) 'Efficiency and enhancement of all relevant structures, processes, and of cooperation in ensuring cyber security', (2) 'Active international cooperation', (3) 'Protection of national CII and IIS',[9] (4) 'Cooperation with [the] private sector', (5) 'Research and development / Consumer trust', (6) 'Education, awareness raising and information society development' (7) 'Support to the Czech Police capabilities for cybercrime investigation and prosecution', and (8) 'Cyber security legislation (development of legislative framework). Participation in creation and implementation of European and international regulations' (NCSS-CZ 2015: 16–20).

The aims should be reached in line with the principles as, for example, the protection of fundamental human rights and the right to freedom, improving human abilities, the attainment of cybersecurity by obeying the principles of subsidiarity, and cooperation at national and international levels.

The strategy makes references to international organizations concerning international cooperation; in particular, the European Union, the North Atlantic Treaty Organization (NATO), and the United Nations Organization are mentioned. Furthermore, it sets forth the need to assist other organizations (with special regard to the Central European area). As far as military cooperation is concerned, the defence-aimed activity of the NATO is written down. The document names actors of economic and scientific sectors because it wishes to develop research and technology hand in hand with the state. Because of the ever-increasing tendency of attacks, establishing efficient security systems has become necessary. The fulfilment of state tasks could be made more operative by the cooperation with people, non-governmental organizations, and the private sector both at domestic and international levels. The state guarantee of secure networks for the population has a significant effect on people's trust in the state. The Czech cybersecurity strategy pays special attention to guaranteeing a democratic legal system, human rights, and the fundamental rights to freedom in the cyberspace.

The term 'challenges' could refer to a number of things: the Czech Republic as a potential test bed; the loss of public trust; the increased number of ICT tools and Internet users; damage caused by technology failures; increase in the number of malware along the growing number of mobile device users; the Internet of Things;[10]

9 Critical Information Infrastructure (CII) and Important Information Systems (IIS).

10 Although desktop computers and laptops are protected by antivirus programs, several other devices connected to the Internet and used in the households have not been secured so far.

the digitalization of public administration; the inappropriate security of small and medium-sized enterprises; the transition from Internet Protocol (IPv4) to Internet Protocol (IPv6); cloud-based data storage; protection of information systems in the health sector and industry; smart networks; increased ICT dependence of state defence forces; more and more sophisticated malware; botnet and DDOS/DOS attacks; cybercrime; challenges related to social networks; the end users' limited digital knowledge; the lack of cybersecurity experts; deficiencies in education.

The document emphasizes the responsibility of the Czech Republic to preserve the security of the elements of the critical infrastructure and the security of networks used by the industry and the population. The National Security Authority (NSA) and the National Cybersecurity Centre (NCSC) are responsible for the regular control, discussion, and evaluation of the aims mentioned in the strategy. The task to prepare an annual report on the cybersecurity situation of the state is assigned to these two authorities. The strategy raises the task of cybersecurity coordination and defence to the national level. Establishing the CERT/CSIRT groups and the cooperation between them is the state's responsibility, more specifically, of GovCERT.CZ.[11]

The Slovak Republic

The Slovak Republic – as in the cases of the Czech Republic and the Republic of Poland – prepared its cybersecurity strategy for a five-year period in 2015, which is the new version of the former one from the year 2008[12] (NCSS-SK 2015). The five chapters specify the principles, the suggested solutions, and the recommendations. The introductory chapter of the document is followed by the explanation of the terms 'cyber' and 'cybersecurity'. The Appendix at the end of the document contains the glossary with some more definitions.

There is a shortage in the cooperation between the state and the private sector, the academic sectors, and the non-governmental organizations; moreover, the coordination system of their cooperation at the strategic level is also missing. The document highlights the need to take steps against challenges and also the need for the secure handling of modern communication technology (it is not defined whose responsibility it should be). Furthermore, the statutory frameworks necessary for the regulation have not been created. The available information security capabilities in the dynamically changing environment are limited for the sake of an efficient and legal defence of public administration and society.

11 GovCERT.CZ is a governmental management unit under the leadership of the National Security Authority (NSA) and the National Cybersecurity Centre (NCSC).

12 Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015–2020 (Cybersecurity Concept of the Slovak Republic for 2015–2020).

The Slovak Republic as a member of the North Atlantic Treaty Organization and the European Union has played an active role in the cybersecurity activities of these organizations and would like to pursue its cooperative activity in the future.

The main goal described in the strategy document is to have an open, secured, and protected cyberspace in order that the critical infrastructures could operate reliably and safely even in case of an attack. To accomplish this, the Slovak Republic formulates several aims to achieve a state where: (1) 'the protection of national cyberspace is a system operating conceptually, in a coordinated manner, efficiently, effectively, and on a legal basis'; (2) 'the security awareness of all components of society is systematically increasing'; (3) 'the private and academic sectors as well as civil society actively participate in the formulation and implementation of the policy of the Slovak Republic in the area of cyber security'; (4) 'efficient collaboration is provided for both national and international levels'; (5) 'the adopted measures are adequate and respect the protection of privacy and basic human rights and freedoms' (NCSS-SK 2015: 9).

The Slovak Republic wishes to put in place a cybersecurity control system that includes institutional, methodological, and regulatory frameworks. Risk control and information exchange between the public and private sectors is necessary. Furthermore, it considers the development of internal market actors dealing with cybersecurity products and services indispensable, and also the support of innovations, research, and development. The document highlights the lack of cyber-specific education (from primary schools to universities), and therefore it orders a methodical cybersecurity education for the educational system.

The (proposed) cybersecurity structure is presented as a standalone figure in the Slovak strategy. It makes the coordinated relationship between the government, the Security Council of the Slovak Republic, the Committee for Cyber Security, the National Security Authority (NSA), and National CERT/CSIRT visible in the supreme decision-making. Their working will be regulated by the Cybersecurity Act. It is the National Security Authority that is responsible for cybersecurity, while the CERT/CSIRT units will be subordinated to the NSA. The strategy defines the tasks, competencies, and entitlements of the CERT/CSIRT units and the sector-oriented authorities.[13]

The document specifies the decision-making and control mechanisms, the prevention mechanisms, the reaction mechanisms, and the restoration mechanisms as basic ones in detail. Intelligence activity is mentioned among prevention mechanisms.

13 Pursuant to the strategy, the National Security Authority is responsible for the following: the preparation of cybersecurity-related tasks and strategy, the supervision of their application; risk management; the development of regulatory frameworks and the methodology of operating measures against cyber attacks for the CERT/CSIRT units; the coordination of action plans of relevant state administration bodies; the coordination and monitoring of task fulfilment; the contacts with the NATO, the European Union, and other international actors.

Hungary

The Hungarian cybersecurity strategy drawn up in 2013 gives a taxonomic description of Hungary's aims, tools, tasks, and environment in four chapters on six pages[14] (NCSS-HU 2013). The document is in line with Hungary's Basic Law, the Hungarian National Security Strategy (Government Regulation No. 1035/2012), the Budapest Convention of the Council of Europe adopted in 2001 (CoE 2001), and the cybersecurity strategy of the European Union and the NATO (EU 2013, NATO 2011).

Among the field-specific terms, it is cyberspace that is given a detailed explanation. Other terms are not explained in the strategy.

The objectives set include the creation of secure and free cyberspace, the protection of national sovereignty at national and international levels. The document also encompasses the guarantee of security of the economy and society – emphasizing the position of children –, the secure adoption and application of technological innovations, and the international cooperation in line with Hungary's interests.

Because attacks launched by states and non-state users are on the rise, the electronic information systems and critical infrastructures need a higher-level protection. Cyberspace is mentioned in the document as one of the main arenas of modern warfare, wherefore the creation of political and professional decision-making is considered necessary. The importance of cooperation between the government and the academic, private, and business sectors regarding security is underlined because these actors have shared responsibility. The Hungarian government cooperates in the global cyberspace with international organizations, with a particular emphasis on the European Union, the NATO, the Organization for Security and Co-Operation in Europe, the United Nations, and the Council of Europe.

The Prime Minister's Office is responsible for the coordination. Incident management is conducted by the Government Incident Response Centre and the Sectorial Incident Response Centres in different sectors. Private, business, and academic sectors should all be involved in preparing the regulation.

Hungary pays attention to the distribution of cybersecurity knowledge in primary, secondary, and higher education[15] as well as public service employees' and specialists' training. The government institutions are to develop a close cooperation with those universities, research institutions that have achieved outstanding and internationally recognized success in the field of cybersecurity.

14 Government Resolution No. 1139/2013 (21 March) on the National Cybersecurity Strategy of Hungary (1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról).

15 In the meanwhile, Hungary established the cybersecurity major in higher education.

Romania

Romania made public its nine-page long cybersecurity strategy over six chapters in 2013[16] (NCSS-RO 2013). The Introduction gives a definition of cyberspace, which is characterized by 'the absence of borders, dynamism, and anonymity' (NCSS-RO 2013: 1). The Romanian state is supposed to have a coordinative role in reaching cybersecurity at the national level. Its activity has to be in line with the European Union and NATO initiatives, with special regard to the security of national critical infrastructure.

The section of the document setting forth objectives uses the term 'virtual environment', in which high-level security has to be reached, in the first place in the case of critical infrastructure. The strategy should support national security and good governance, which is supposed to be for the benefit of the population and the business/corporate sector as well as the whole of Romanian society.

Additional goals mentioned in the document include:

a) adapt the regulatory and institutional framework to the cyberspace threats dynamics;

b) establish and implement security profiles and minimum requirements for national cyber infrastructures, relevant in terms of the proper functionality of the critical infrastructures;

c) ensure the resilience of cyber infrastructure;

d) ensure security through understanding, preventing and fighting vulnerabilities, risks and threats to cyber security of Romania;

e) take advantage of the opportunities to promote the national interests, values and objective in the cyberspace;

f) promote and develop cooperation between the public and private sectors at national and international level in the field of cybersecurity;

g) develop a security culture by raising awareness of the population concerning the vulnerabilities, risks and threats originating from cyberspace and the need to ensure protection of their information systems;

h) active participation in the initiatives of international organizations which Romania is part of in defining and establishing a set of international confidence-building measures concerning use of cyberspace. (NCSS-RO 2013: 2)

The secure cyberspace is listed as an objective both in Romania's National Defence Strategy and the National Strategy for the Protection of Critical Infrastructure. That is the reason why the cybersecurity strategy was created in compliance with the two documents mentioned.

16 Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acțiune la nivel național privind implementarea Sistemului național de securitate cibernetică (the cybersecurity strategy of Romania).

The strategy defines seventeen cyberspace-related terms (cyberspace, cyber defence, cybersecurity, cyber-attack, cyber threat, cyber incident, cyber espionage, cybercrime, cyber infrastructure, security risk, cyber terrorism, cyber vulnerability, risk management, CERT-type entity, identity management, cyber infrastructure resilience, and operations in computer networks). Cyberspace is defined as a virtual environment that has been created by the cyber infrastructure, including the formation, storage, and transmission of information, and the users' activity related to these operations.

The document underlines that Romania has to seriously face threats against cyber infrastructure. This is justified by substantial interdependence between the cyber infrastructure and, for example, the banking system, the energy sector, and the national defence sector. The risks concern the population, the business sector, and public service.

The attacks are launched by actors that could be individuals, organized crime groups, terrorists, or extremists, state-related or non-state actors. The strategy distinguishes three possibilities regarding the cyberspace attacks: cybercrime, cyber terrorism, and cyber warfare. All three of them could have state- or non-state origins and could be carried out in several forms:

1. cyber-attacks against the infrastructure supporting public functions or information society services, whose disruption or damage could constitute a danger to the national security;
2. unauthorized access to cyber infrastructures;
3. modification, deletion, or deterioration of computer data or unauthorized illegal restriction of access to such data;
4. cyber espionage;
5. causing patrimonial damage, harassing, and blackmailing individuals and businesses, public and private. (NCSS-RO 2013: 4)

The National Cybersecurity System (NCSS) provides the general framework for cooperation between the authorities and institutions (research institutions, universities, professional and non-governmental organizations, etc.) in cybersecurity at the national level. Its main aim is to avert and prevent attacks, vulnerabilities, and risks that could affect the national cyber infrastructure, including consequence management. There are proactive and reactive measures formulated in the NCSS: first of all, sharing of cyber-specific knowledge, information distribution, data recovery, and implementation of cybersecurity strategy. Its efficiency depends on the cooperation between the public and private sectors.

The Supreme Council of National Defence[17] is the coordinating actor at a strategic level regarding the operation of the National Cybersecurity System. The Supreme Council of National Defence approves the state's cybersecurity strategy and the policies and procedures of the Cybersecurity Operative Council. Using the Ministry of Communication and Information Society, the government of Romania coordinates the work of authorities that are not members of the Cybersecurity Operative Council.

The task of the CERT-RO (Computer Emergency Response Team Romania) is to fulfil the national cybersecurity policy in that incidents are thwarted and prevented by its actions.

The strategy pays close attention to cooperation between business and private sectors and international organizations (e.g. the European Union, the North Atlantic Treaty Organization, Organization for Security and Co-operation in Europe, etc.).

Comparative Analysis

The content of the documents analysed is similar in several points because all of them are based on the Cybersecurity Strategy of the European Union (EU 2013), the NIS directives (NIS 2016), and the ENISA guidelines, and the Cybersecurity Strategy of the NATO was taken into account by the five states as well. Nevertheless, some differences are noticeable among the objectives and measures.

All five documents consider cybersecurity a pivotal factor of state security. However, they differ in length: the Slovak strategy has 31, the Polish 26, the Czech 23, the Romanian 9, and the Hungarian 6 pages. In the case of the first three documents, attention was also paid to the format because the authors completed them with a title page and a table of contents. The Czech and Slovak documents have spectacular design elements too. The Slovak strategy document uses the term 'Incident Resolution Unit' instead of the EU-wide accepted 'Computer Security Incident Response Team'.

Table 3 contains the publishing date of the analysed strategies, the number of objectives set, and data regarding CERT/CSIRT units.

Hungary pays the least attention to clarify cyber-related terms; only the term cyberspace is explained in its strategy. Slovakia, Poland, and the Czech Republic prepared an extra glossary and a list of abbreviations.

17 Members of the Supreme Council of National Defence are the Ministry of National Defence, Ministry of Internal Affairs, Ministry of Foreign Affairs, Ministry of Communication and Information Society, the Romanian Intelligence Service, Special Telecommunication Service, the Foreign Intelligence Service, Protection and Guard Service, the National Registry Office for Classified Information, and the Secretary of the Supreme Council of National Defence.

Table 3. *Summary of particular features of cybersecurity strategies adopted by Romania and the V4 countries*

	Czech Republic	Hungary	Slovakia	Poland	Romania
NCSS	2011, 2015	2013, 2018	2008, 2015	2013, 2017	2013
Year of establishment for the Computer Emergency Response Teams – CERTs	2011	2013	2009	2016	2013
Number of objectives	8	5, 9	5	4	8
Number of CSIRT (Computer Security Incident Response Team)	28	3	7	11	6
Offensive cyber-capability in the NCSS	no	no	no	yes	no

Source: the cyber security strategies of the 5 countries, own research

All five documents prioritize the defence of the state and highlight the cooperation with international and national actors; the former group is represented chiefly by the European Union and the NATO. The Polish strategy includes a goal concerning offensive cyber capability, while the others only have goals of a defensive character. The further goals listed include preparation for the attacks, their countering, setting up specialized organizations (CERT/CSIRT) for incident investigation and management. Beyond the defence of critical infrastructures, the defence of business actors and the population are also equally represented in all strategies. The Czech Republic particularly emphasizes the industry and healthcare. Slovakia makes references to intelligence among preventive measures, whereas the other states do not mention intelligence services in their documents.

There is a significant overlap of the measures referring to the defence of public, critical infrastructures, the business sector, and non-governmental organizations, and it is necessary to have a cooperation between national and international actors.

Summary

Nowadays, cybersecurity is one of the main challenges states have to face. This should be reflected in the strategies, too. The analysis shows that this has come true in the case of the countries examined.

The threats from the cyberspace have arisen in enormous extent and have become sophisticated. They have been lifted to the state level and have called for a strategy formation as well as defence measures at national and international levels. Besides their similarities, the cybersecurity strategies of the five Central European countries show some differences in their goals and defence measures. These similarities and differences have been described by this paper with an aim to help experts verify and prepare strategic documents.

References

CLXVI. 2012. *The Hungarian Law about the Identification, Attribution, and Defence of Critical Infrastructure No. CLXVI*. https://net.jogtar.hu/jogszabaly?docid=a1200166.tv (Downloaded on: 23.10.2020).

CoE. 2001. *Budapest Convention. Convention on Cybercrime*. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 (Downloaded on: 23.10.2020).

CSIKI, Tamás. 2008. A stratégiai dokumentumok rendszere. *Nemzet és Biztonság* 1(8): 76–81. www.nemzetesbiztonsag.hu/cikkek/csiki_tamas-a_strategiai_dokumentumok_rendszere.pdf (Downloaded on: 23.10.2020).

DESI. 2020. https://digital-strategy.ec.europa.eu/en/library/digital-economy-and-society-index-desi-2020 (Downloaded on: 18.8.2021).

ENISA. 2016. *NCSS Good Practice Guide. Designing and Implementing National Cyber Security Strategies*. European Union Agency for Network and Information Security. ISBN: 978-92-9204-179-3 DOI: 10.2824/48036.

EU. 2013. *EU Cybersecurity Strategy: An Open, Safe and Secure Cyberspace*, P7_TA-PROV(2013)0000 (europa.eu) (Downloaded on: 23. 10. 2020).

EUROSTAT. 2021. https://ec.europa.eu/eurostat/web/population-demography/demography-population-stock-balance/database (Downloaded on: 18.8.2021).

GCI. 2021. *Global Security Index (GCI).* ITU. https://www.itu.int/epublications/publication/global-cybersecurity-index-2020/en/ (Downloaded on: 18.8.2021).

ITU. 2020. https://www.itu.int/en/Pages/default.aspx (Downloaded on: 23.10.2020).

KOVÁCS, László. 2018. *A kibertér védelme*. Budapest: Dialóg Campus. ISBN 978-615-5889-64-6. (Downloaded on: 23.10.2020).

MIHAI, Ioan-Cosmin–CIUCHI, Costel–PETRICĂ, Gabriel. 2018. *Current Challenges in the Field of Cyber Security. The Impact and Romania's Contribution to the Field. European Institute of Romania*. ISBN 978-606-11-6575-9.

NATO. 2011. *NATO Policy on Cyber Defence*. https://www.nato.int/nato_static/assets/pdf/pdf_2011_08/20110819_110819-policy-cyberdefence.pdf. (Downloaded on: 23.10.2020).

NCSS-CZ. 2015. *National Cyber Security Strategy of the Czech Republic for the Period from 2015 to 2020*. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-of-czech-republic-2011-2015 (Downloaded on: 23.10.2020).

NCSS-HU. 2013. *Government Decision No. 1139/2013 (21 March) on the National Cyber Security Strategy of Hungary*. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy and http://njt.hu/cgi_bin/njt_doc.cgi?docid=159530.238845 (Downloaded on: 23.10.2020).

NCSS-PO. 2017. *National Framework of Cyber Security Policy of the Republic of Poland FOR 2017–2022.* https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/govermental-program-for-protection-of-cyberspace-for-the-years-2011-2016-2013 (Downloaded on: 23.10.2020).

NCSS-RO. 2013. *Cyber Security Strategy of Romania*. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-in-romania (Downloaded on: 23.10.2020).

NCSS-SK. 2015. *Cyber Security Concept of the Slovak Republic for 2015–2020*. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-concept-of-the-slovak-republic (Downloaded on: 23.10.2020).

NIS. 2016. OJ EU 2016 L194 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:194:FULL&from=NL (Downloaded on: 23.10.2020).

WEF. 2013. Global Risks 2013. 8th edition. http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2013.pdf (Downloaded on: 2020.10.23).