Anna Urbanovics[1]

Cybersecurity Strategies in the Visegrád Countries – A Cross-Country Analysis[2]

The European Union is one of the most developed regions with regard to its cyber policy. While 14 out of the top 15 countries based on the National Cybersecurity Index are European countries, the Central European region is in a semi-peripheral position being less developed in cybersecurity policy. The paper aims to evaluate four of these countries – namely the Czech Republic, Hungary, Poland and Slovakia – often referred to as "Visegrád" countries, based on their cybersecurity policy. The region is geopolitically exposed to cyberattacks, however, only Poland follows a military approach in cyber policy development. The methodology is based on a mixed approach, consisting of the quantitative analysis of the countries based on international databases and a qualitative strategy analysis. The results indicate that the Czech Republic leads among the countries of the region. Although the countries of the region concentrate on the fight against cybercrime and personal data protection, other indicators such as the contribution to global cybersecurity policy allow further development.

Keywords: *Visegrád countries, militarisation, cybersecurity, strategy analysis, cyber policy development*

Introduction

Central European countries and within them especially the Visegrád countries – namely the Czech Republic, Hungary, Poland and Slovakia – form a special group of countries based on similar historical path and similar geopolitical conditions. In the field of security and defence policy, they are active participants in both the North Atlantic Treaty Organization (NATO) and the European Union (EU). Nowadays, due to the growing number of cyberattacks and the ever-widening type of cyber threats, cybersecurity has become an integral part of the defence policy of a country and an important domain of national interests. Cybersecurity is often identified in the international literature as "the technologies, processes, and policies that help prevent and/or reduce the negative impact of events in cyberspace that can happen as the result of deliberate actions against information technology by a hostile or malevolent actor".[3]

[1] PhD student, University of Public Service. E-mail: anna.urbanovics@gmail.com

[2] The present publication was presented in an oral form on the *II Military Science and Military Art International Conference* at the Ludovika University of Public Service, Budapest, Hungary, on 14 October 2022. Project no. TKP2021-NVA-16 has been implemented with the support provided by the Ministry of Innovation and Technology of Hungary from the National Research, Development and Innovation Fund, financed under the TKP2021-NVA funding scheme.

[3] Clark, David – Berson, Thomas – Lin, Herbert S. eds. (2014): *Computer Science and Telecommunications Board. At the Nexus of Cybersecurity and Public Policy.* Washington, D.C.: The National Academy Press.

In recent years, we can see that cyberattacks are on the rise, as stakeholders are often not prepared to tackle these issues. This could be observed during the Covid-19 pandemic and the Ukrainian war that began in February 2022. Countries are exposed to cyberattacks and more specific national-level policy development is needed. However, European countries stand out from this respect based on the world ranking of the National Cybersecurity Index (14 out of the top 15 countries are European), the Visegrád countries still lag behind compared to the Western European countries.

This paper aims to provide an overview on a comparative basis, involving quantitative and qualitative tools, about the national cybersecurity policies of the four Visegrád countries – the Czech Republic, Hungary, Poland and Slovakia.

The paper is divided into six sections. After the introduction, the second chapter deals with the militarisation of cyberspace and the relevance of national cybersecurity strategies. Then, the methodology of the paper is presented. In the fourth section, the digital adoption level of the studied countries is summarised, while in the fifth section the results of the comparative analysis are summarised. Following these, in the sixth section conclusions of the research are listed.

The militarisation of cyberspace and the development of national cybersecurity policies

As we could see from the world ranking of the National Cybersecurity Index, European countries are among the leaders in national cyber policy and preparedness.[4] The NCSI database was chosen as the primary database of the current comparative analysis due to its holistic view on national cybersecurity policies and achievements, also due to its evidence-based data collection and methodology. Although cyber threats do not have a unified definition, due to their different nature, safeguarding national security in cyberspace has become crucial for these countries.[5] Some key concepts need to be clarified. Building a comprehensive cyber policy requires "cybersecurity governance" referring to "a holistic and integrated vision of the security of networks, systems, services, and infrastructures in society. It includes the institutions, initiatives, policies, programs, and other mechanisms (formal and informal) that are part of an ecosystem of distributed capacities and responsibilities regarding cybersecurity".[6] As a result, a cybersecurity strategy is launched in countries which can be defined as "a political manifestations of the country subscriber to the extent that your content tends to divide responsibilities among national stakeholders, stipulate the strategic objectives pursued, define goals, furthermore, in the country, concrete steps should be achieved within defined deadlines and the potential threats perceived by the country should be identified".[7]

[4] National Cybersecurity Index. [online], e-Governance Academy Foundation, s. a. Source: ncsi.ega.ee [12.10.2022].

[5] Świątkowska, Joanna ed. (2012): *V4 Cooperation in Ensuring Cyber Security – Analysis and Recommendations.* Krákow: Koscluszko Institute.

[6] Hurel, Louise Marie (2021): Cybersecurity in Brazil: An Analysis of the National Strategy. *Igarapé Institute, Strategic Paper 54,* April 2021.

[7] Luiijf, Eric et al. (2013): Nineteen National Cyber Security Strategies. *International Journal of Critical Infrastructure Protection,* 9(1–2), 3–31.

In the 2010s, cyberspace as a new domain of war emerged. In 2016, NATO recognised it as a domain of military operations. Countries use their capabilities in cyberspace that leads to the "characterization of the digital environment as a martial "cyber" domain".[8]

The European Union is active in the cybersecurity field as well. In 2017, the EU reaffirmed its "commitment to the peaceful settlement of international disputes in cyberspace" and it focuses on stability and reducing misunderstandings arising from the use of ICT tools. In this effort, it actively shapes cyber diplomacy.[9] The EU lacks the offensive cyber capabilities, therefore its approach to cybersecurity derives from the protection of fundamental rights and economic interdependence both at a global and intra-EU level.[10] It is important to note that among EU member states, the Visegrád group has established active cooperation in the field of cybersecurity and cyber diplomacy.[11]

There are two main concepts how cybersecurity issues can be perceived by states. The so-called national security paradigm highlights the role of the state in guaranteeing the borders of the countries and the application of the rule of law within its territory.[12] Following this logic, cybersecurity is a multifaceted policy area that establishes cybersecurity that requires states to secure public, private and economic cyber activities.[13] Cybersecurity is considered fundamental to the military and economic security of a state and is approached as such with traditional national security arguments based on protecting the homeland. In contrast to the military concept, the civil approach regards cybersecurity as a matter of economic interests, as the Internet plays a key role in economic development and welfare of the country.[14] From this approach, the creation of a comprehensive cybersecurity policy requires the participation of different stakeholders and the public–private partnership. Among the studied countries, Poland follows the military approach, while the Czech Republic, Hungary and Slovakia follow the economic approach in cybersecurity policy development.[15]

In alignment with the securitisation theorists (referred to as Copenhagen school),[16] there is a growing dependence of nations on cyber infrastructure, therefore cybersecurity issues have become securitised.[17] The securitisation concept suggests that the

[8] Zittrain, Jonathan (2017): 'Netwar': The Unwelcome Militarization of the Internet Has Arrived. *Bulletin of the Atomic Scientists,* 73(5), 301.

[9] Molnár, Anna (2022): A kiberdiplomácia fejlődése az Európai Unióban. In Molnár, Anna – Molnár, Dóra (eds.): *Kiberdiplomácia.* Budapest: Ludovika University Press. 55–72.

[10] Kasper, Agnes et al. (2021): Ciberseguridad y ciberdiplomacia de la UE. *IDP,* 34, 1–15.

[11] Tikos, Anita (2022): Cyber Diplomacy and the V4 Countries. In Molnár, Anna – Mártonffy, Balázs (eds.): *Cyber Diplomacy from the European Perspective.* Budapest: Ludovika University Press. 129–150.

[12] Newmeyer, Kevin P. (2015): Elements of National Cybersecurity Strategy for Developing Nations. *National Cybersecurity Institute Journal,* 1(3), 9–19.

[13] Harknett, Richard – Stever, James A. (2009): The Cybersecurity Triad: Government, Private Sector Partners, and the Engaged Cybersecurity Citizen. *Journal of Homeland Security and Emergency Management,* 6(1).

[14] Newmeyer 2015: 9–19.

[15] Tomic, Dusko et al. (2018): Cyber-Security Policies of East European Countries. In Carayannis, Elias – Campbell, David – Efthymiopoulos, Marios (eds.): *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense.* Cham: Springer. 1039–1055.

[16] Buzan, Barry et al. (1998): *Security. A New Framework for Analysis*. Boulder: Lynne Rienner.

[17] Lobato, Luísa Cruz – Kenkel, Kai Michael (2015): Discourses of Cyberspace Securitization in Brazil and in the United States. *Revista Brasileira de Política Internacional,* 58(2), 23–43.

materialisation of this process is highlighted through an analysis of policies and institutional and strategic responses. Thus, it is important to analyse how states, acting as securitising actors, become alert to the risks of cyberattacks and then establish a specific agenda to deal with threats. In this context, maintaining a secure cyberspace legitimises the use of extraordinary measures.

Methodology

The methodology used in the paper is based on comparative quantitative analyses. It can be divided into two parts. It is important to note here that the quantitative analyses based on international indexes provides a solid background for data analysis, because they use the same methodology and evaluation form in every case;[18] therefore, the positions of the objects of the analyses relative to each other give reliable result. First, basic indicators introduced a general picture of the selected countries, including individual-specific and country-level indicators. These can be found in the general overview section of the study. Then, a more detailed quantitative analysis was conducted using the National Cybersecurity Index (NCSI).[19] The National Cybersecurity Index is a global index, which measures the preparedness of countries to prevent cyber threats and manage cyber incidents. The NCSI is also a database with publicly available evidence materials and a tool for building national cybersecurity capacity. The development process of the NCSI database consists of 5 steps (Figure 1).

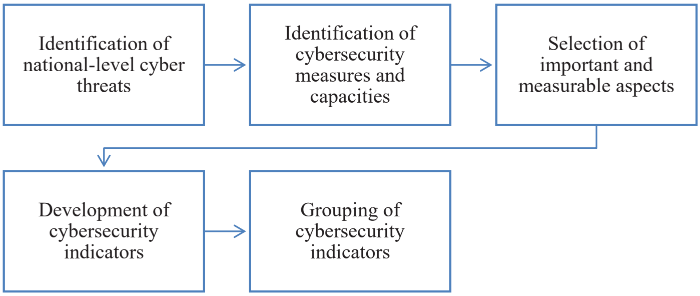

Identification of national-level cyber threats
Identification of cybersecurity measures and capacities
Selection of important and measurable aspects
Development of cybersecurity indicators
Grouping of cybersecurity indicators

Figure 1: Steps of the development process of the National Cyber Security Index database

Source: Compiled by the author based on the information provided by the NCSI.

The database focuses on the measurable aspects of cybersecurity implemented by the national central governments, including the legislations in force, the established units, the cooperation formats and the outcomes. It collects evidence in three categories, 12 capacities and 46 indicators.

[18] Bolgov, Radomir: *The UN and Cybersecurity Policy of Latin American Countries.* 2020 Seventh International Conference on eDemocracy and eGovernment (ICEDEG). 259–263.

[19] National Cybersecurity Index s. a.

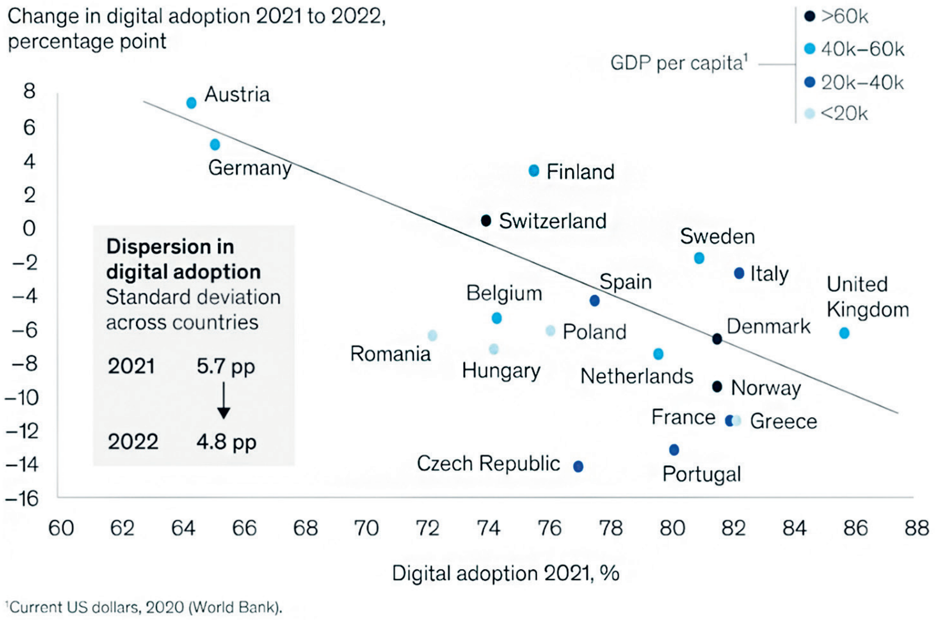
A qualitative document analysis has been carried out as well, based on national cybersecurity strategies as follows:

- The Czech Republic: National Cyber Security Strategy of the Czech Republic 2021–2025
- Hungary: Government Decision No. 1139/2013 (21 March) on the National Cyber Security Strategy of Hungary
- Poland: Cybersecurity Strategy of the Republic of Poland for 2019–2024
- Slovakia: The National Cybersecurity Strategy 2021–2025

The database includes data about the Czech Republic as of 4 February 2020, about Hungary (13 October 2022), about Poland (21 December 2020) and Slovakia (6 July 2020). The legislation and cited data are included in the database, here they will not be placed in the reference list.

The digital adoption of the Visegrád Countries

Before studying the national cybersecurity developments in the Visegrád countries, we should study the more general digital context of these countries. This helps to highlight the countries' preparedness for the implementation of the cybersecurity policy.



[1] Current US dollars, 2020 (World Bank).

Figure 2: The change in digital adoption 2021 to 2022 and the digital adoption level of European countries

Source: Hajro et al. 2022

The IMD World Digital Competitiveness Index[20] measures the countries' digital competitiveness worldwide based on three pillars, including knowledge, technology and future readiness. According to the 2022 report, we can see that the studied Central European countries are among the top 50 countries in each pillar, led by the Czech Republic in overall (33rd place in the world ranking), followed by Hungary (42nd place), Poland (46th place) and Slovakia (47th place). Regarding the pillars, the Czech Republic leads in the knowledge pillar (32nd place) and the future readiness pillar (29th place), while Hungary achieved a higher ranking in the technology pillar (31st place).

After studying digital competitiveness, it is worth checking the country-level digital adoption as well. Based on a recent report (June 2022) launched by McKinsey & Company, there is a correlation between the level of digital adoption and the GDP per capita in European countries. Higher the GDP per capita, higher the level of digital adoption, including Denmark, Finland, Sweden, Switzerland, while the lower the GDP per capita, the lower the level of digital adoption, for example, in case of the Czech Republic, Hungary and Poland. During the Covid-19 pandemic, as we can see in the figure (Figure 2), there were some countries falling back in digital adoption, including the Czech Republic, Hungary and Poland. Based on the results of the Global Digital Sentiment Insight Survey, there are significant differences between sectors in digital adoption. The sector-specific results are summarised in Table 1 (note here that data about Slovakia are not available).

Table 1: The sector-specific change in digital adoption 2021 to 2022

	The Czech Republic	Hungary	Poland
Education	–23	–26	–19
Retail	–11	–15	–7
Public sector	–8	–4	–4
Healthcare	–8	–6	–20
Travel	–7	–14	–13
Insurance	–6	–4	0
Utilities	–5	–9	–3
Entertainment	–3	–5	–2
Grocery	–2	0	–4
Telco carriers	0	–3	2
Banking	1	1	1
Average	–5	–7	–6

Source: Compiled by the author based on Hajro et al. 2022

We can see that, on average, the biggest decrease was in Hungary (–7%). The most significant drops can be observed in education (26% in Hungary), in retail (15% in Hungary), in healthcare (20% in Poland) and in the travel sector (14% in Hungary). The banking sector is the only one where improvement could be achieved in terms of the level of digital development between 2021 and 2022.

[20] IMD World Digital Competitiveness Index. [online], International Institute for Management Development, s. a. Source: imd.org [03.12.2022].

Comparative analysis of cybersecurity developments

The National Cyber Security Index and the Digital Development Index provide overall indicators for comparative analysis. To focus on every aspect of these two pillars, however, goes beyond the framework of the present study.

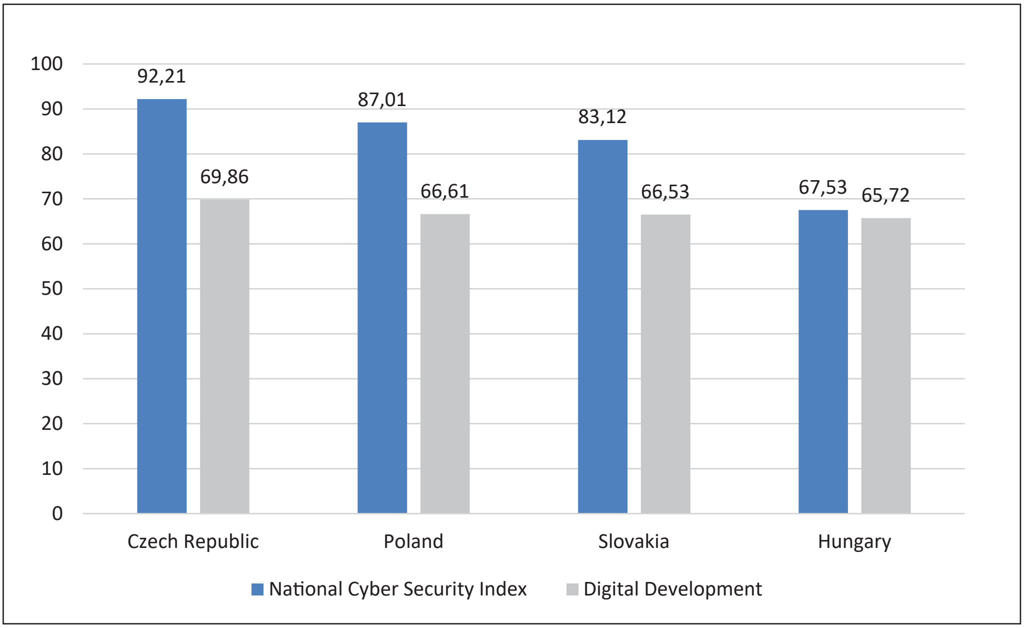


Figure 3: Ranking of the countries by the National Cyber Security Index and Digital Development Index

Source: Compiled by the author based on the information provided by the NCSI.

The database of the National Cybersecurity Index provides two general indicators – namely the National Cyber Security Index and the Digital Development Index – to measure the preparedness of the national cyber policies of countries in a complex way (Figure 3). From both aspects, the Czech Republic stands out, with 92.21 points in the National Cyber Security Index and 69.86 points in the Digital Development. At the second place regarding the NCSI we find Poland (87.01 points), while in the Digital Development, we find Hungary (65.72 points). The countries show a relatively high preparedness according to the NCSI, but there is room for further development in the Digital Development. On the global ranking, the Czech Republic takes the fifth place, followed by Poland (10th place), Slovakia (17th place) and Hungary (35th place).

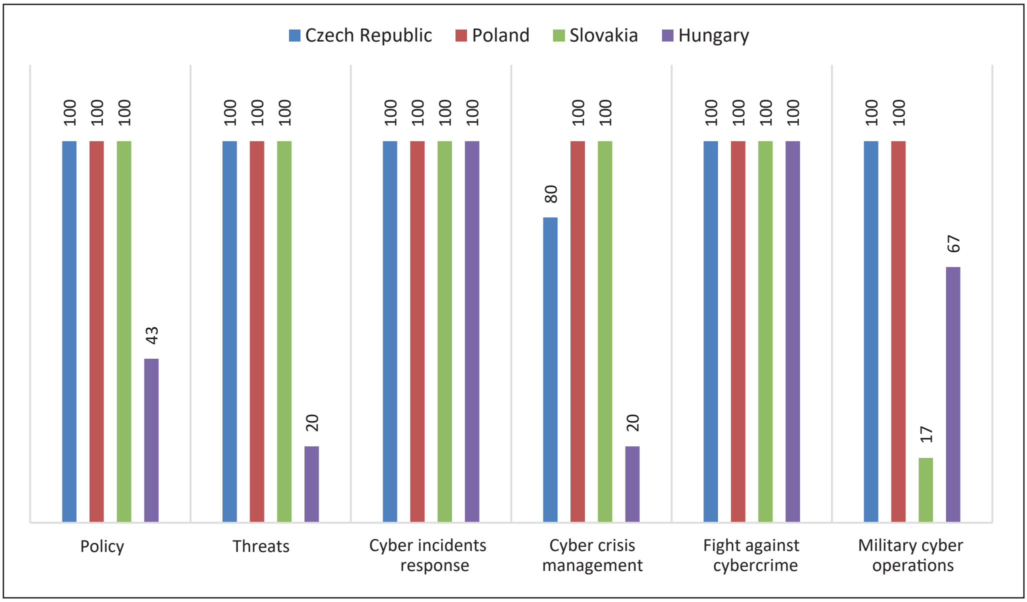


Figure 4: Evaluation of the Visegrád countries based on policy-related indicators of the National Cyber Security Index

Source: Compiled by the author based on the information provided by the NCSI.

In the analysis, the altogether 12 indicators will be divided into two sets of indicators. The first set of indicators is rather related to the political and defence dimensions of cybersecurity, and the cybersecurity policy in general (Figure 4).

The cyber incident response and fight against cybercrime indicators are equally developed in every country studied, they have already reached full potential according to the NCSI database. Regarding the cyber incident response, the countries have an established unit – namely the CERT and CSIRT in the Czech Republic, the NCSC unit in Hungary, CERT in Slovakia, and a collection of 3 CIRTs at national level (CSIRT NASK, CSIRT GOV, CSIRT MON) in Poland. In addition, digital service providers and operators of essential services have an obligation to report cyber incidents, while the governments provide a single point of contact for international cyber coordination. In every country, cybercrimes are criminalised by the national law; the first country to include cybercrime in their national Penal Code was Slovakia in 2005 among them, followed by the Czech Republic in 2009. The countries provide a list on what they consider a cybercrime, in Hungary, for example, these are as follows:

- illegal access to information system
- illegal system interference
- illegal data interference
- illegal interception of computer data
- misuse of devices

Regarding cyber crisis management, Poland and Slovakia stand out, having a cyber crisis management plan, having organised national-level cyber crisis management exercise, participating in international cyber crisis exercises, and providing operational support of volunteers in cyber crises. In Slovakia, the National Cyber Security Centre (SK-CERT) has conducted national table-top exercises, focused on cyber crisis management for various subjects, while in Poland cross-sectoral cybersecurity exercises took place in 2017 (LIBERO 2017) and 2019 (LIBERO 2019).

Regarding the military cyber exercises, the Czech Republic and Poland stand out, both having a cyber operations unit, an organised cyber operations exercise at national level, and participated in an international military cyber operation. In Slovakia, the cyber operation unit has not been established yet, but they have already participated in international cyber military operation, while Hungary is somewhat more developed because the only missing aspect is that the country has not organised a national level cyber operation. All of these countries are active in international military cyber operations; a list is as follows:

- The Czech Republic: Cyber Coalition 2017, Locked Shields 2017, Locked Shields 2019
- Hungary: EU MilCERT Interoperability Conference (MIC) 2021–2022, Locked Shields 2021
- Poland: Cyber Coalition 2018, Crossed Swords 2019, Locked Shields 2019
- Slovakia: Cyber Coalition 2017

Further details are summarised in Table 2 on the legislative framework and structure of these countries in their cyber policy. The countries became FIRST[21] members in different periods, starting with Poland in 1997, followed by Hungary in 2006, the Czech Republic in 2015 and Slovakia in 2018. The date of joining the FIRST network shows the different maturity of national cyber policies. We can see some differences with respect to the national cybersecurity strategy as well, the earliest still relevant strategy is in Hungary (compiled in 2013), then in Poland in 2019 for the period of 2019–2024, and the latest can be found in the Czech Republic and Slovakia for the period 2021–2025. Every country has its own national-level central administrative entity, in the Czech Republic as a form of agency, in Hungary a coordination council, while the two other countries handle cybersecurity within a more complex ministerial entity.

[21] The FIRST is an international network bringing together incident response and security teams from every country across the world to ensure a safe internet for all. It aims to provide platform and tools for collaboration.

Table 2: Main elements of national cybersecurity policy

Country	Strategy documents	Dedicated agency	Summary of responsibilities	National CERT/ CSIRT	FIRST membership
Czech Republic	• The Defence Strategy of the Czech Republic 2017 • National Cyber Security Strategy of the Czech Republic 2021–2025 • The Prague Proposals: Cyber Security of Communication Networks in a Globally Digitalized World • How to Approach 5G Policies • Implementation and Development of 5G Networks in the Czech Republic • 2020 Report on Cyber Security in the Czech Republic	National Cyber and Information Security Agency	Serves as central administrative body for cyber security, including the protection of classified information in information and communication systems and cryptographic protection. Responsible for the implementation of the public regulated service of the global navigation satellite system under the Galileo programme.	CSIRT (CSIRT.CZ)	2015 (CSIRT.CZ)
Hungary	• National Cyber Security Strategy of Hungary (No. 1139/2013) • Cyber Defence Concept of the Hungarian Defence Forces • National Security Strategy (No 1163/2020)	National Cyber Security Coordination Council	Responsible for planning, regulation, control and incident handling.	CERT (govCERT)	2006 (govCERT)
Poland	• Cybersecurity Doctrine of the Republic of Poland • Cyberspace Protection Policy of the Republic of Poland • National Security Strategy Of The Republic Of Poland 2020 • Cybersecurity Strategy of the Republic of Poland, 2019–2024	Ministry of Digital Affairs	Its main tasks are to develop broadband infrastructure, support the creation of web content and e-services and promote digital competences among citizens.	CERT Polska CSIRT GOV CSIRT MON	1997 (CERT Polska)
Slovakia	• Cyber Security Concept of the Slovak Republic (2015–2020) • White Paper on Defence of the Slovak Republic • National Strategy for Information Security in the Slovak Republic • National Cybersecurity Strategy 2021–2025	National Security Authority	It is the central government body for Protection of Classified Information, Cryptographic Services, Trust Services and Cyber Security. Manages and coordinates carrying out of state administration. Determines the standards, operational procedures, issues the methodology and policy of behaviour in cyberspace; Determines the principles for preventing cybersecurity incidents and principles for their handling; Elaborates the National Cybersecurity strategy and the annual report on the state of cybersecurity in the Slovak Republic in cooperation with the respective state authorities.	CERT (SK-CERT)	2018 (SK-CERT)

Source: Compiled by the author based on the data of the UNIDIR Cyber Policy Portal.

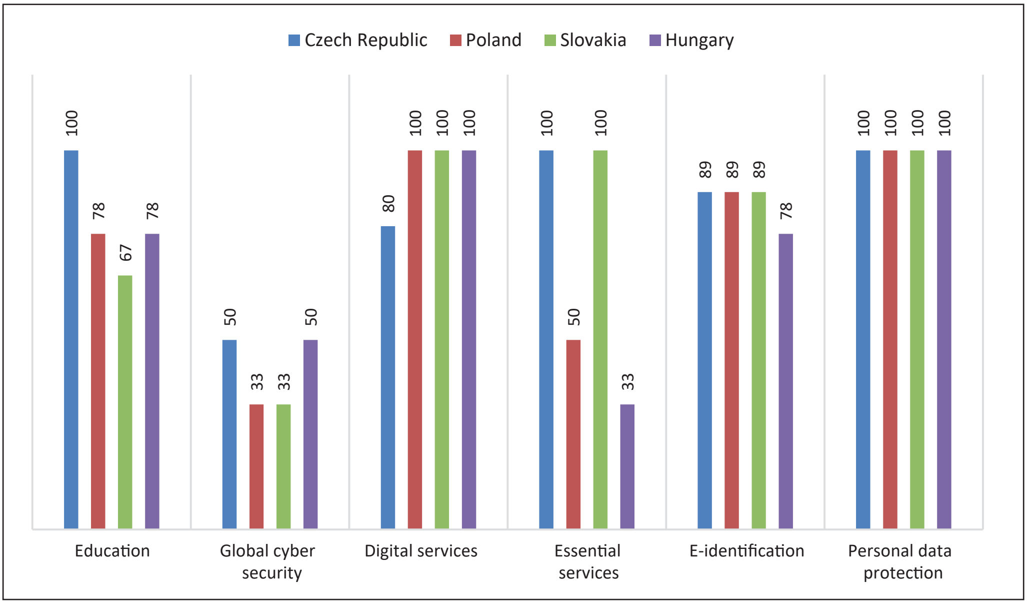


Figure 5: Evaluation of the Visegrád countries based on data protection-related indicators (National Cyber Security Index)

Source: Compiled by the authors based on the data of the NCSI

The second set of indicators is mainly related to services and data protection issues (Figure 5). Among them, the personal data protection is the most developed in these countries. All of them have established and enacted national regulations and set up the authority specialised in data protection issues. As all of them are member states of the European Union, the GDPR[22] applies, too. In the Czech Republic, the Office for Personal Data Protection (an independent body) tackles data protection issues based on Act 110/2019 Coll. In Hungary, the National Authority for Data Protection and Freedom of Information, in Poland, the Personal Data Protection Office, and in Slovakia, a supervisory authority responsible for all essentials on data protection, the Office for Personal Data Protection is the main entity. As we can see, the protection of digital services and essential services are relatively developed indicators as well. However, the protection of essential services, in Poland, the competent supervisory authority, in Hungary, the same authority, and a regular monitoring of security measures is absent.

Regarding education, the Czech Republic offers the most comprehensive opportunities in cybersecurity education including cyber safety competencies in primary or secondary schools, Bachelor's, Master's and PhD level degree programs, and cybersecurity professional certificates. In Hungary, the Bachelor's level degree program, in Poland the PhD

[22] The General Data Protection Regulation (2016/679, "GDPR") is a Regulation in EU law on data protection and privacy in the EU and the European Economic Area.

level degree program, while in Slovakia the cyber safety competencies in primary and secondary school and PhD level degree programs are missing.

The countries studied perform relatively low – compared to the other indicators – in the contribution to global cybersecurity. In an attempt, Hungary contributed to the development of cyber capacity of Uganda within the framework of an International Development Programme in the Republic of Uganda. The title of the program was *Enhancing Local IT Capacities and Capabilities*. Cybersecurity threats pose one of the greatest challenges to developing countries and modern economies alike. Therefore, Hungary implemented a "specially designed cybersecurity development project in Uganda with the aim of enhancing local defence capacities and capabilities. The project included the establishment of a Malware and Forensic Analysis Laboratory, in addition to the provision of the necessary trainings. The project was completed in May 2020".[23]

Similarly, the Czech Republic participated in Africa-related programs as well – namely the Africa Endeavour Symposium organised by the U.S. Africa Command from 30 July to 3 August 2018 and from 19 to 23 August 2019.

After the index-based quantitative comparison, it is worth studying the national cybersecurity strategies of these countries from a qualitative approach. Here, the emphasis is put on the vision and mission of the strategies and the strategic objectives. Common points can be found in all four strategies; however, compared to the complex nature of the other three, Hungary's strategy does not include so many details. It is important to note, however, that in Hungary a new cybersecurity strategy is under progress currently. The vision in each country is built around strategic cooperation and alliances and the encouragement of a resilient information society. The Czech strategy states these as follows: "The Czech Republic will have a resilient society and infrastructure, will act confidently in cyberspace, and will actively confront the entire spectrum of cyber threats while strengthening reliable alliances." The Slovak strategy is in some way broader: "The vision of the National Strategy is to strengthen and create an open, free, and secure cyberspace for everyone." In the Hungarian strategy, cybersecurity is defined as a national interest and a key element in maintaining the country's sovereignty. "The protection of Hungary's sovereignty in the Hungarian cyberspace is also of national interest, too; a free, democratic, and secure functioning of the Hungarian cyberspace based on the rule of law is regarded as a fundamental value and interest. In Hungary, the freedom and security of cyberspace is ensured through the close cooperation and coordinated activities between Government, academia, business sector, and civil society based on their shared responsibility." The Polish strategy focuses more on the information systems and safe operation in cyberspace, as follows: "The efficient and safe operation of information systems and means of electronic communication contributed to the successful growth of the Republic of Poland, the increasing the effectiveness of the economy and performance of institutions and entities, also including its social activity and everyday functioning of individual members of the society. Therefore, as part of the actions planned in the Cybersecurity

[23] Hungary's International Development Programme in the Republic of Uganda. [online], International Development Cooperation, 2019. Source: nefe.kormany.hu [03.12.2022].

Strategy, by the year 2024, the government shall systematically enhance and develop the national cybersecurity system."

Parallel with these, strategic objectives are set in national strategies. These objectives have several focus points that can be found in every strategy, including the national-level cyber capacity building, public awareness and education, promoting the development of research innovation in cybersecurity, preparing a resilient private sector, enhancing the public–private partnership, and actively engaging with the international partners to create strong partnerships abroad.

Conclusions and perspectives

Due to the growing number of cyberattacks in recent years, the NATO and EU has already established a focused cybersecurity policy based on the trust and collaboration of member states. This helps member states become competitive and many times leaders in cybersecurity policy not just regionally but worldwide. These tendencies are reflected in the IMD Digital Competitiveness report as well. However, during the Covid-19 pandemic there was a serious decline in most of the sectors related to digital adoption.

The studied region – namely the Czech Republic, Hungary, Poland and Slovakia – forms a semi-periphery regarding the maturity of their cybersecurity national policies, although the countries have already taken promising steps and have quite mature cybersecurity strategies. The Czech Republic stands out among them both with regard to the National Cybersecurity Index score and the Digital Development scores. However, these countries are among the most developed ones regarding defence-related cybersecurity policy indicators – mainly in cyber incident response and the fight against cybercrime, room for further development can be found related to service and data protection indicators, and the contribution to global cyber policy.

Regarding future scenarios, these countries must rethink their geopolitical conditions mainly in light of the Ukrainian war and include a stronger military approach – following the example of Poland – in the cybersecurity policy.

REFERENCES

Bolgov, Radomir (2020): *The UN and Cybersecurity Policy of Latin American Countries.* 2020 Seventh International Conference on eDemocracy and eGovernment (ICEDEG). 259–263. Online: https://doi.org/10.1109/ICEDEG48599.2020.9096798

Buzan, Barry – Wæver, Ole – de Wilde, Jaap (1998): *Security. A New Framework for Analysis.* Boulder: Lynne Rienner. Online: https://doi.org/10.1515/9781685853808

Clark, David – Berson, Thomas – Lin, Herbert S. eds. (2014): *Computer Science and Telecommunications Board. At the Nexus of Cybersecurity and Public Policy*. Washington, D.C.: The National Academy Press.

Cybersecurity Strategy of the Republic of Poland for 2019–2024. [online], Ministry of Digital Affairs, 2019. Source: mc.bip.gov.pl [03.01.2022]

Government Decision No. 1139/2013 (21 March) on the National Cyber Security Strategy of Hungary. [online], Government of Hungary, 2013. Source: kormany.hu [03.01.2022]

Hajro, Neira – Hjartar, Klemens – Jenkins, Paul – Vieira, Benjamim: Opportunity Knocks for Europe's Digital Consumer: Digital Trends Show Big Gains and New Opportunities. [online], McKinsey Digital, 28 June 2022. Source: mckinsey.com [03.12.2022]

Harknett, Richard – Stever, James A. (2009): The Cybersecurity Triad: Government, Private Sector Partners, and the Engaged Cybersecurity Citizen. *Journal of Homeland Security and Emergency Management,* 6(1). Online: https://doi.org/10.2202/1547-7355.1649

Hungary's International Development Programme in the Republic of Uganda. [online], International Development Cooperation, 2019. Source: nefe.kormany.hu [03.12.2022]

Hurel, Louise Marie (2021): Cybersecurity in Brazil: An Analysis of the National Strategy. *Igarapé Institute, Strategic Paper 54,* April 2021.

IMD World Digital Competitiveness Index. [online], International Institute for Management Development, s. a. Source: imd.org [03.12.2022]

Kasper, Agnes – Osula, Anna-Maria – Molnár, Anna (2021): Ciberseguridad y ciberdiplomacia de la UE. *IDP,* (34), 1–15. Online: https://doi.org/10.7238/idp.v0i34.387469

Lobato, Luísa Cruz – Kenkel, Kai Michael (2015): Discourses of Cyberspace Securitization in Brazil and in the United States. *Revista Brasileira de Política Internacional,* 58(2), 23–43. Online: https://doi.org/10.1590/0034-7329201500202

Luiijf, Eric – Besseling, Kim – De Graaf, Patrick (2013): Nineteen National Cyber Security Strategies. *International Journal of Critical Infrastructure Protection,* 9(1–2), 3–31. Online: https://doi.org/10.1504/IJCIS.2013.051608

Molnár Anna (2022): A kiberdiplomácia fejlődése az Európai Unióban. In Molnár, Anna – Molnár, Dóra (eds.): *Kiberdiplomácia.* Budapest: Ludovika University Press. 55–72.

National Cyber Security Strategy of the Czech Republic 2021–2025. [online], NÚKIB, 2021. Source: nukib.cz [03.12.2022]

National Cybersecurity Index. [online], e-Governance Academy Foundation, s. a. Source: ncsi.ega.ee [12.10.2022]

Newmeyer, Kevin P. (2015): Elements of National Cybersecurity Strategy for Developing Nations. *National Cybersecurity Institute Journal,* 1(3), 9–19.

Świątkowska, Joanna ed. (2012): *V4 Cooperation in Ensuring Cyber Security – Analysis and Recommendations.* Krákow: Koscluszko Institute.

The National Cybersecurity Strategy 2021–2025. [online], National Security Authority, 2021. Source: nbu.gov.sk [03.01.2022]

Tikos, Anita (2022): Cyber Diplomacy and the V4 Countries. In Molnár, Anna – Mártonffy, Balázs (eds.): *Cyber Diplomacy from the European Perspective.* Budapest: Ludovika University Press. 129–150.

Tomic, Dusko – Šaljić, Eldar – Cupic, Danilo (2018): Cyber-Security Policies of East European Countries. In Carayannis, Elias – Campbell, David – Efthymiopoulos, Marios (eds.): *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense.* Cham: Springer. 1039–1055. Online: https://doi.org/10.1007/978-3-319-09069-6_59

UNIDIR Cyber Policy Portal. [online], United Nations, s. a. Source: cyberpolicyportal.org [03.12.2022]

Zittrain, Jonathan (2017): 'Netwar': The Unwelcome Militarization of the Internet Has Arrived. *Bulletin of the Atomic Scientists,* 73(5), 300–304. Online: https://doi.org/10.1080/00963402.2017.1362907