Trustworthy cybersecurity cooperation of Visegrád countries

Nguyen Huu Phuoc Dai[1], Zoltán Rajnai[2,*]

[1]Doctoral School on Safety and Security Sciences, Óbuda University, Budapest, Hungary
[2]Bánki Donát Faculty of Mechanical and Safety Engineering, Óbuda University, Budapest, Hungary

Received: 17 October 2021; Accepted: 15 December 2021

Summary

In Europe, every country has its national security strategy, particularly in the area of cybersecurity. Furthermore, each nation has its own set of circumstances, powers, technological advancements, and rules. Cooperation and a unified approach can prove difficult. As a consequence, this article examines the cooperation of Visegrád countries and other organizations in the field of cybersecurity from the perspective of cybersecurity experts, as well as the official V4 legal framework and national sources to identify the differences and similarities of Visegrád countries' strategies. Besides, the authors aimed to uncover solutions on how to maintain their power in the same location and develop the strength of the EU and other organizations.

Keywords: cooperation, cybersecurity, cybersecurity strategies, V4, Visegrád

A visegrádi országok megbízható kiberbiztonsági együttműködése

Nguyen Huu Phuoc Dai[1], Rajnai Zoltán[2,*]

[1]Óbudai Egyetem, Biztonságtudományi Doktori Iskola, Budapest, Magyarország
[2]Bánki Donát Gépész és Biztonságtechnikai Kar, Óbudai Egyetem, Budapest, Magyarország

Összefoglalás

Európában minden országnak megvan a maga nemzeti biztonsági stratégiája, különösen a kiberbiztonság területén. Ezenkívül minden nemzetnek megvannak a saját követelményei, technológiai fejlődései és szabályai. Az együttműködés és az egységes megközelítés nehéznek bizonyulhat. Ebből kifolyólag ez a cikk a visegrádi országok (V4) és más szervezetek kiberbiztonsági együttműködését vizsgálja a kiberbiztonsági szakértők szemszögéből, valamint a hivatalos V4 jogi keretek és nemzeti források segítségével azonosítja a visegrádi országok stratégiáinak különbségeit és hasonlóságait. Emellett a szerzők arra törekedtek, hogy megoldásokat találjanak arra, hogyan tartsák fenn jelentőségüket, és erősítsék az EU és más szervezetek erejét.

Kulcsszavak: együttműködés, kiberbiztonság, kiberbiztonsági stratégiák, V4, visegrádi országok

1. Introduction

In the 14th century, three kings – John of Luxembourg, Charles Robert, and Casimir III of the Czech Republic, Hungary, and Poland – gathered in Visegrád on the Danube (Hungary) to sign an alliance contract *(Musil 2011)*. The summit's major goal was to collaborate on commerce, taxation, and trade routes. Moreover, this cooperation served as a mini-model for the future of the European Union. Many events took place between the Visegrád nations after nearly a century of collaboration. Following the Warsaw Pact, three delegates from three nations met for the first time in Bratislava on 9th April 1990 and signed the Declaration on Cooperation between them and Slovakia on 15th February, 1991 to join into European integration – the so-called V4 group. This cooperation mainly targeted to enhance their power in the same region and develop the EU and other Member States in many aspects. This article mainly focuses on figuring out the trustworthy cooperation of Visegrád countries, especially in cybersecurity. Moreover, the authors indicated the way how V4 maintains its strength in the same region.

1.1. Why Visegrád countries cooperate?

The Visegrád nations have significant similarities including the region's historical evolution, culture, economics, society, geography, and security issues *(Helšusová 2003);* thus, there is a potential natural collaboration for the future enhancement of the Central European area *(Brazova–Matczak–Takacs 2013)*. Each of the V4 countries has acknowledged the importance of cybersecurity challenges, cyber dangers, and the urgent need to defend their citizens' security. They also protected their democracy, civil rights, information secrecy, and privacy *(Kirňák et al. 2017)*. Visegrád cooperation has the following objectives: restoration of the sovereignty of the country, democracy and freedom, elimination of the remnants of the totalitarian system, and so on. Furthermore, Visegrád nations are tiny Eastern European countries with a combined territory of around 500,000 km^2 and a population of 60 million people, which is almost equal to the area and population of France. On the other hand, the number of V4 troops is around 200,000 soldiers, which is comparable to that of Germany or the UK *(Musil 2011)*. Moreover, the most essential critical element for collaboration is the countrys' entrance to the European Union in 2004 and other international organizations. In addition, the Visegrád nations envisaged an organization that would stand for extensive interactions among them, especially in terms of geographical, historical, and cultural commonalities, as well as the hurdles posed by former communist countries *(Kirňák et al. 2017)*. Hence, the cooperation of the Visegrád countries has created a strong regional organization in Europe.

1.2. The system of V4

The presidency of V4 changes for each country annually. Each president puts together his/her program to ensure the long-term cooperation for V4. There are several meetings between the V4 Presidency and other ministers in V4 and V4+ format. In addition, some meetings between the Presidents and the Parliament of these nations are held annually. V4 has the major tasks to maintain contact and cooperation with the Permanent Representations to the EU and NATO, as well as the OSCE, UN, COE, the OECD, the WTO, and the like. Even though there are a lot of shared goals and common interests, each V4 cybersecurity strategy is fragmented in different ways *(Table 1)*.

Table 1. | Fragmentation authorities of Visegrád countries

Country	Authorities
CZECH REPUBLIC	– Cyber Security managed by the Ministry of Interior (2010–2011) – National CERT (CSIRT.CZ) – CZ.NIC – legal entities operation in (domain name, e-communication market) – CERT (GOVECERT.CZ) – Military CERT/CIRC administered by the Ministry of defense (armed forces, defense ministry) – 20 private CERTs
SLOVAKIA	– National CERT/CSIRT – CSIRT.SK response in the civil sector – Ministry of finance. CSIRT.SK cooperates with a similar team on the international platform on a regional level with the teams of V4 and Austria – CSIRT.MIL.SK – for monitoring, evaluation, measure-taking of information security
POLAND	– Strategic/policy level by Ministry of digital affairs with the Ministry of finance, justice, interior – National Center for cybersecurity and national CERT/CSIRT with sectoral CERTs/CSIRTs (energy, financial, banking, water supply, administration, etc.) – Technical level including SOC (security operations center) – Ministry of finance responsible for cybersecurity issues – Ministry of defense used for national security, military security – Ministry of Interior responsible for critical infrastructure
HUNGARY	– At the government level (National cybersecurity council supported by national cybersecurity forum, academic & business sector council, some task-oriented workgroups) – Ministry of interior – for central governmental incident management, Critical Infrastructure – National CIRT (or GovCERT) – Ministry of defense – for military incident management (MilCERT) – National Directorate general – for disaster management – Hungarian internet service providers – providing civil domain – NIIF institute – NIIF CSIRT workgroup to protect Hungarian mid- and higher education and research sector – GovCERT and MilCERT – tend to keep secrets instead of sharing data

Source: authors' own compilaton

2. The Visegrád countries' cooperation

2.1. Cooperation among V4 nations

V4 cooperate in some areas such as culture, education, science, infrastructure, environment, and youth exchange. In addition, the Visegrád countries also extend the experience of transformation in the areas of terrorism prevention, organized crime, refugees, disaster management, and the defense industry. The V4 also cooperate in disaster management, infrastructure, or the environment. Likewise, they are strengthening the development of defense and armament industries to fight back the terrorists.

2.2. Cooperation with EU

V4 nations are mainly active contributors to the EU in developing the Common Foreign and Security Policy (CFSP) and the EU strategy towards the Western Balkans and participate in the development of the European Security and Defense Policy (ESDP) to enhance EU relations with NATO. Visegrád cooperation creates new opportunities and forms of economic cooperation within the European Economic Area and discusses preparations for the use of the European Monetary Union (EMU). After participating in the EU and NATO, the V4 also helped the Western Balkan countries in improving the integration process of the Western Balkans and the Euro-Atlantic including several practical assistance in 2014, e.g. in the fields of law, children's rights, public space, and administrative reform. Due to the migration crisis, in 2016 there was a meeting between the Ministers of Interior of the V4, Slovenia, Serbia, and Macedonia to improve the control of migration flow. In addition, the V4 also cooperated with the Benelux Group in 2003 in eight important areas to clarify possible joint actions and contribute to strengthening the common foreign, security, and defense policy of the EU. Likewise, the V4 is currently working with Austria and Germany (V4+) to improve stability, reduce cyber threats to peace, and build Euro-Atlantic security relations with NATO and other partner countries.

2.3. Cooperation with the other international organizations

Visegrád is expanding cooperation with other partners that have similar interests with the main goals to strengthen transatlantic solidarity and cohesion, to promote a common understanding of security between the EU countries and the Euro-Atlantic area, to improve the fight against international terrorism, to exchange information in international organizations (UN, Council of the EU, OECD, etc.) and to consult in the OSCE on issues of common interest to the V4 countries. With the boosting of ICT, V4 members face many challenges from cyber threats. Hence, Austria and V4 began to cooperate in 2013 with the creation of the Central European Cyber Security Platform (CECSP). The cooperation's purpose of the five states is to enable the

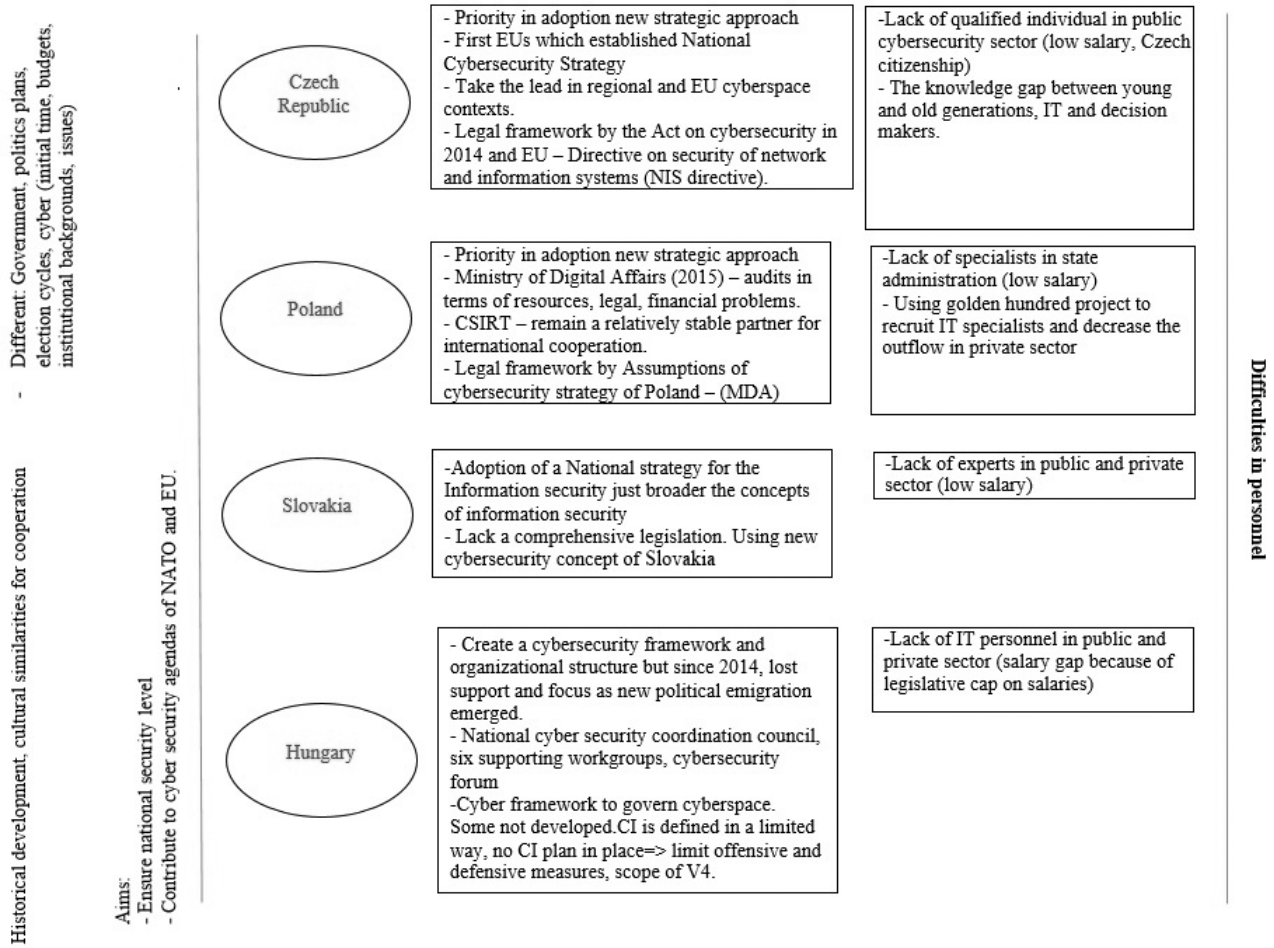

Figure 1 V4 cybersecurity strategies

Source: authors' own compilaton

information, best practices, lessons learned, and know-how sharing about cyber threats and potential solutions for cyber-attacks *(Berzsenyi 2015)*. Moreover, this platform will provide the capacity and capability building in improving the V4 position in the international environment. Besides, V4 also take part in Digital Three Seas Initiative cooperation for economic growth, development IoT, Artificial Intelligence (AI), 5G, digital infrastructure, tactical cooperation against cyber threats and disinformation *(Kosciuszko 2018)*.

3. Cybersecurity strategies of Visegrád countries, similarities and differences

Although V4 nations have many common interests and cyber threats, several similarities and dissimilarities in their cybersecurity strategies are described in *Figure 1*.

Furthermore, the Ministry of Interior is in charge of Hungary, the Czech Republic, and Slovakia's cybersecurity strategy, and they have civil resilient cooperation. In contrast, Poland has cybersecurity capabilities belonging to the Ministry of Military. Also, Hungary and national cybersecurity institutions focus on civilian law capabilities and it belongs to the Ministry of Interior and civilian security services. As a result, because the former is on the Interior side and the latter is on the Military side, Hungarian and Polish cyber center groups cannot collaborate. The internal cybersecurity of V4 has offense power by law or regulations. They established the CPPP cooperation as well as close cooperation with the Universities. While Poland and the Czech Republic have power in CERT, Slovakia and Hungary are still in their infancy in terms of cyber-attack protection. Moreover, the Czech Republic differs from the other three nations in that it has legal offense powers.

4. Is this cooperation good?

The V4 collaboration demonstrated that it was a good potential partnership at international and political levels. This connection is based on a shared history, geographical proximity, economic partnership, and knowledge of public interests *(Małecki 2018)*. Based on their shared objectives, the V4 not only improves the EU and NATO's security structures but also cyber defense more effectively, functionally, and powerfully. Currently, one of the critical issues is the immigration situation that requires V4 collaboration in supporting the admission process alongside the EU. In addition, regarding this cooperation, it can help them in resolving energy challenges since they rely on importing energy. These concerns include a lack of an integrated energy market, infrastructure, and interruptions in supplying energy supplies. Furthermore, in the face of comparable cyber threats, V4 collaboration may boost military capabilities and cooperation among the armed forces by exchanging military exercises, fighting skills, and defensive experiences. Poland, for example, is developing army cyber-attack capabilities. While the Czech Republic is good at not only in technological fields but also in cybersecurity, Hungary excels in engineering education, and Slovakia surpasses with a public-sector cybersecurity leader *(Davis 2017)*. On the other hand, they can support each other to proactively defend against cyber-attacks and improve the global cybersecurity index for each member by year from 2017 to 2020 *(Figure 2)*. Likewise, based on the five major pillars of digital life: (internet affordability, quality, e-infrastructure, e-security, and e-government) *(Davis 2017)*, this cooperation can encourage its digital space for both residents and businesses of each member. For example, in comparison to 110 countries in the world, Hungary ranked 32nd , Czech Republic 28th, Slovakia 29th, and Poland 25th *(Surfshark 2021)*.

Visegrád countries	Global Rank
Poland	34
The Czech Republic	35
Hungary	51
Slovakia	82

a

Visegrád countries	Global Rank
Poland	30
The Czech Republic	68
Hungary	35
Slovakia	34

b

Figure 2 Global cybersecurity index in 2017 (a) and Global cybersecurity index in 2020 (b)

Source: ITU 2017, 2022

5. Conclusion

This article has briefly covered the Visegrád nations' founding (history, the purpose of cooperation, and its mechanism). Besides, it also demonstrated how the V4 nations collaborated within the V4, as well as with the EU and other international organizations (NATO, Western Balkans, Benelux group, OECD, and UN). Moreover, the authors also described an overview of the similarities and differences between the V4 members in cybersecurity tactics. Regarding the benefits of the V4 collaboration described above, the authors indicated that these nations are recognized as one nation with a significant influence on the EU and NATO in boosting cybersecurity, cyber defense, and other critical concerns such as immigration issues and energy.

References

Berzsenyi, D. (2015) New dimension of V4. http://visegradplus.org/analyse/new-dimension-v4-defense-cooperation-comparative-analysis-cybersecurity-strategies-cecsp-countries/

Brazova, V. K., Matczak, P, & Takacs, V. (2013) Regional Organization Study: Visegrad Group. Anvil (Analysis of civil security systems in Europe) . Poznań, Adam Mickiewicz University in Poznań.

Davis, J. (2017) Slovakia's Leadership in Public Sector Cybersecurity Will Benefit the Visegrád Group and Beyond. https://research-center.paloaltonetworks.com/2017/12/cso-slovakias-leadership-public-sector-cybersecurity-will-benefit-visegrad-group-beyond/

ITU (2017) Global Cybersecurity Index & Cyberwellness Profiles 2017. https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E/

ITU (2022) Global Cybersecurity Index 2020. https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E/

Kirňák, M., Šulc, R., Illési, Zs., & Gapiński, K. (2017) V4 Goes Cyber: Challenges and Opportunities. https://www.yumpu.com/en/document/read/56535184/v4-goes-cyber-challenges-and-opportunities

Małecki, M. (2018) V4: 'It's good to be among friends'. The Warsaw Institute Review. https://warsawinstitute.org/v4-good-among-friends/

Musil, M. (2011) Visegrad Group – After 20 years. Economic Review, Vol. 40. No. 4, pp. 429–447. [Online]. https://www.euba.sk/www_write/files/SK/ekonomicke-rozhlady/er4_2011_Musil-9564.pdf

Orosz, A. (2017) The Western Balkans on the Visegrad Countries' Agenda. KKI Policy Brief. Series of the Institute for Foreign Affairs and Trade, E-2017/39. https://kki.hu/assets/upload/39_KKI_Policy_Brief_V4-WB_Orosz_20171214.pdf

Surfshark (2021) Digital Quality of Life Index. https://surfshark.com/dql2021 (accessed 17 Nov, 2021)

The Kosciuszko Institute (2018) Digital 3 Seas Initiative cooperation". https://ik.org.pl/en/projects/thedigital3seasinitiative/

Václavíková Helšusová, L. (2003) Visegrad cooperation as seen by the citizens of four countries. In Gyárfášová (ed.) Visegrad citizens on the doorstep of European Union. https://www.visegradgroup.eu/download.php?docID=53