Anita Tikos

Cyber Diplomacy and the V4 Countries

Introduction

If we think about diplomacy, it is commonly understood as a task of the Ministries of Foreign Affairs to influence decisions, conduct dialogues and negotiations between representatives of states or international groups, forums. Due to the digital development, in the 21st century, the use of IT solutions and tools in diplomatic services became more and more widespread starting from public relations and information sharing, to data collection for intelligence purposes. In view of all this, it is more and more important to establish common rules, code of conducts, security related requirements within the cyberspace.

We can find several different meanings and definitions for cyber diplomacy. In this article, cyber diplomacy is understood, when country representatives (not only form the Ministry of Foreign Affairs, but from any governmental cyber related institution) share information, conduct dialogues or negotiations regarding any cybersecurity related topic (about an incident, about existing regulatory or organisational experiences, common EU regulations, exercises, etc.) in general (not going deeply into restricted or sensitive technical details).

The Central European Cyber Security Platform (CECSP) is a regional cooperation where members use strategic cooperation or cyber diplomacy to get the necessary information, experience or knowledge from the other countries and to get enough support to be able to effectively promote their interests in the bigger international communities.

First, I would like to introduce the development of the international forums and cooperation to get a full picture about the colourful palette of the different international cooperation platforms and forums where CECSP was born.

In the last decade, cybersecurity has appeared as a key challenge for all countries and organisations, resulting in the establishment of organisations or divisions that are responsible for the creation and maintenance of information

https://doi.org/10.36250/01039_06

security (e.g. authorities, CSIRTs,[1] Security Operation Centres, cyber defence agencies or centres of excellence, etc.). Due to the possible cross-border nature of threats and incidents, it became relatively clear at an early stage that there is a need for international forums and mechanisms for the structured international cooperation of the specialised IT security organisations.

Regarding cybersecurity, cooperation is one of the most important and at the same time the most challenging issues for every country. Although it is essential for all entities in the cyberspace to get relevant information on the latest threats but giving such threat intelligence for others usually encounters obstacles because of several aspects (for example national and security interest, data protection aspects etc.).

First, a technical international cooperation has been established by setting up communities of incident management centres (CERT[2]/CSIRT); after the CSIRT communities the political, strategic cooperation has been established in different forms (groups of authorities, strategic working groups by decision-makers, etc.). As of today, the main international organisations (NATO, EU, ITU, OSCE) all put cybersecurity on their agenda.

This wide list of international cooperation is always growing because of the different cooperation models (who are the involved players) and because of the developing technology (technology creates new and new policy areas) as well.

In 2013, the Czech Republic and Austria has enriched this huge cooperation with initiating the establishment of the Central European Cyber Security Platform or CECSP as a new regional cooperation. The regional agreement has created strategic and operational cooperation between the four Visegrád countries (the Czech Republic, Hungary, Poland, Slovakia), as well as Austria. The regional cooperation of the Central European countries is not a completely new initiative; there was another similar regional cooperation initiative like the CECSP, the so-called Central European Defence Cooperation (CEDC) established in 2011, aiming to facilitate the military-focused collaboration. Maybe the CECSP is the next step or the extension of the CEDC as all of the CECSP members are also members of the defence cooperation (Poland only as an observer). But it is important to highlight that the CEDC itself was not involved in the latter established CECSP cooperation, but as we will see later, the military cyber groups were also involved in it. There is only one similar, regional defence platform in

[1] Computer Security Incident Response Team.

[2] Computer Emergency Response Team.

Europe, NORDEFCO, founded by the Nordic countries, but it does not have a specific, cybersecurity-oriented agreement.[3]

The question may arise, considering that CECSP countries are participating in several already existing organisations, why do we need a regional cooperation, and what new role can be played by the CECSP in strategic or operational level cooperation. Is it possible to reach real operational cooperation or it is rather a strategic and diplomatic level regional cooperation?

To find the possible answers, I will give an overview on the cybersecurity policy of the platform's member states and their goals and activities in the cyberspace. I will present the history of the CECSP cooperation and its relations to the V4 cooperation and to the EU level regulation: *Directive on Security of Network and Information Systems* (NIS Directive). This study was prepared by using and updating an earlier case study: *Cybersecurity in the V4 Countries – A Cross-border Case Study.*[4]

The Cybersecurity Structure of CECSP Countries

Countries that are members of the platform participate in the cyberspace related work of the major international communities without exception. As the cybersecurity regulations of these communities are developing into the same direction and their members must implement these regulations, the CECSP countries have essentially similar legal and organisational structures.[5]

It is important to emphasise that before the *Directive on Security of Network and Information Systems* (NIS Directive) had been adopted in 2016, only guidelines and strategic objectives from international organisations and studies or guides about best practices showed examples internationally; therefore, the legal and organisational system of the countries was quite different.[6]

[3] Bence Németh: *Outside NATO and the EU. Sub-Regional Defence Co-Operation in Europe.* London, King's College, 2017.

[4] Anita Tikos – Csaba Krasznay: *Cybersecurity in the V4 Countries – A Cross-border Case Study.* Central and Eastern European e|Dem and e|Gov Days 2019. 163–174.

[5] Dániel Berzsenyi: Kiberbiztonsági analógiák és eltérések. A Közép-európai Kiberbiztonsági Platform részes országai által kiadott kiberbiztonsági stratégiák összehasonlító elemzése. *Nemzet és Biztonság,* 7, no. 6 (2014).

[6] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union.

To understand and clearly see the full picture about the regional cooperation, it is worth comparing the cybersecurity preparedness and system of the countries that are members of the platform based on their national strategy and organisation system. It will not be a detailed strategic and organisational analysis; the aim is only to highlight the main similarities and differences by drawing up a comprehensive picture.

The first national cybersecurity strategies were established at about the same time by the CECSP countries in the early 2010s. The Czech Republic was the first who published a national strategy on cybersecurity in 2008, then Slovakia in 2011, and finally Austria, Poland and Hungary, all in 2013.[7]

Of course, over the years these strategies have been reviewed, because the period of their effect has expired and/or the development of the technology brought new challenges to cover.

Therefore, Slovakia and the Czech Republic formulated their new second generational national strategy for the period 2015–2020, meanwhile Poland published its own in 2017.

After the NIS Directive was adopted, it became the obligatory model for all future strategy of every country. These principles do not have new strategic elements compared to the existing international practice, but this is the first time when these are not just optional elements of the national strategies.

Hungary found a special solution to comply with these requirements; as the strategy accepted in 2013 is a general one and the main aims are still valid, Hungary extended this cybersecurity strategy with the Network and Information Systems Security Strategy of Hungary in 2018, which is a "so-called" sectoral strategy.[8] As the title suggests, this sectoral strategy covers the main strategic requirements of the NIS Directive.

Poland decided to strengthen and develop systematically its national cybersecurity system while implementing the EU cybersecurity regulatory framework

[7] Government of Hungary: Government Decision No. 1139/2013 (21 March) on the National Cyber Security Strategy of Hungary. *ENISA,* 21 March 2013; Republic of Austria: *Austrian Cyber Security Strategy.* 10 March 2013; Government of Poland: National Framework of Cybersecurity Policy of the Republic of Poland. *ENISA,* 30 November 2017; Government of the Slovak Republic: Cyber Security Concept of the Slovak Republic. *ENISA,* 01 June 2015; Government of the Czech Republic: National Cyber Security Strategy of the Czech Republic for the Period from 2015 to 2020. *ENISA,* 16 January 2015.

[8] Government of Hungary: Government Decision No. 1838/2018 (28 December 2018) on Hungary's Strategy for Network and Information Security.

(including the NIS Directive and Cyber Act); therefore, a new Cybersecurity Strategy of the Republic of Poland for 2019–2024 has been accepted.[9] The strategy of Slovakia and the Czech Republic was valid and has aims until 2020, so they published their third strategy in late 2020 and at the beginning of 2021.

The Czech Republic defined its new strategy for 2021–2025 in January 2021.[10] This strategy will continue to fulfil the vision of the previous strategy but with new solutions to the new threats. The most important aspect of the strategy is the resiliency and the capacities of state security services, state institutions, organisations and individuals. This strategy does not mention the NIS Directive, and does not define any definite regulatory or organisational process/requirement or change. The effective international cooperation is one of the aims of the strategy, and within this point the cooperation of the Central European region is also mentioned as one international cooperation platform where they plan to strengthen the country's active role. The resilient society 4.0 is one of the main aims of this strategy, where securing the digital society and public administration, education and awareness raising and expanding the qualified cybersecurity workforce are the main aims. On the other areas, the main aim is to strengthen the resilience, capacity building, preventing and fighting cybercrime, better information sharing and cooperation, define communication strategy and update its national regulations to be able to effectively react to new challenges, threats, etc.

The new Slovak strategy, the National Cyber Security Strategy 2021–2025 defined the strategic aims for the next five year. This strategy continues the concept and aims of the previous strategy, plus tries to address the new threats and challenges in a modern way to be able to respond to the constantly evolving cyber threats and cybersecurity, it defines the principles of the cybersecurity system to ensure a higher level of security in the cyberspace of the Slovak Republic. This strategy mentions the NIS Directive, but does not aim to implement it, as the implementation period has already expired. This strategy has several ambitious aims in the field of international cooperation (in different international organisations and in bilateral cooperation), but it does not mention the CECSP cooperation at all. Austria still does not publish a new strategy since 2013, or

[9] Republic of Poland: Uchwała Nr 125, Rady Ministrów w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024. 12 October 2019.

[10] National Cyber Security Center (NCKB): National Cyber Security Strategy of the Czech Republic for the Period from 2021 to 2025. *NUKIB,* 18 March 2021.

any assessment about the compliance of the strategy with the requirements of the NIS Directive and the new threats and challenges within the cyberspace.

We can say that all national strategies (every generation) of all five countries include the relevant areas from international (ENISA, NATO, ITU) cybersecurity strategy guidance, such as objectives for education, research and development, awareness-raising, public–private partnership, law enforcement, international cooperation and critical infrastructure protection.

In case of the first and second generational strategies, they vary from the legislative perspective. Some of the strategies aims at the creation or the update of a comprehensive information security regulation (in case of Slovakia or Poland), while for other countries they refer specifically to the legal regulation of one or two areas in the strategy paper (for example in the case of Hungary).

Regarding cybersecurity organisations, it must be highlighted that all evaluated strategies identify the governmental and/or national incident management centre (GovCERT/national CERT), the regulatory body with rights and responsibilities and the organisation or ministry responsible for coordination and for decision-making.[11]

There is a discrepancy between the strategies – in the first two generations – regarding the non-governmental areas (for example: regarding the critical infrastructure sectors), and in the organisational coverage. The other difference is that the development of regulations and the creation of specialised organisations can be observed only as a goal in some sectors, while in other cases the critical infrastructure and/or sectoral regulations are already existing, and the goal is to strengthen and further develop them.

Each evaluated strategy deals with the question of non-governmental, sectoral CERTs and the establishment of military CERTs. The countries have a same approach in terms of the need for the creation of special sectoral CERTs, but they are in different stages in the implementation. In Austria, there are many commercial CERTs operating and the country has a military CERT (MilCERT), whereas in Hungary and the Czech Republic one of the objectives is the establishment of a sectoral CERT.

Each strategy highlights the importance of the active international cooperation, mainly referring to the European Union and NATO, but in several cases the regional cooperation (or especially the Central European cooperation) has been highlighted as a priority.

[11] Lászó Kovács: *Kiberbiztonság és -stratégia.* Budapest, Dialóg Campus, 2018.

Regarding the third generational strategies, we can say that they cover the same main elements, sectors and institutional requirements but they still vary in detail (regarding their priorisation and the chosen legal and organisational solutions in detail). In the Hungarian sectoral strategy, one important aim is to strengthen the international and regional cooperation.

In the new Polish, and Czech strategy, the active international cooperation at the strategic and political level is also an important aim, where the Central European cooperation is also mentioned as an important cooperation platform, but the new Slovak strategy does not have any aim or reference to the CECSP at all.

It is important to know that the strategies cannot be used to draw a conclusion on the similarity or differences of the organisational structures, as a number of organisational development and transformation took place in the countries during the adoption of their strategies, that cannot be read out directly from the strategy itself, such as the creation of commercial CERTs or the military CERTs. For example, in Hungary the organisational structure has changed several times, and the main changes in the last 5 years (for example: in 2015, the National Cyber Security Center, so-called NCSC was set up by uniting 3 existing cybersecurity related organisations, or the Defense Sector Electronic Information Security Incident Management Center – MilCERT was established on 1 March 2016) was also not covered directly by the national cyber strategy but still supports the implementation of the strategic aim to create the necessary specialised cybersecurity related institutions:

In conclusion, the national strategies have shown us that the CECSP countries have similar priorities and timelines at strategic level, and the international and regional cooperation is an important aspect for every country since the beginning.

The Historical Background and the Main Aims of the Central European Cyber Security Platform

In accordance with the fundamental objectives of the CECSP countries, the main aims of the thematic regional cooperation are to work together in accordance with the guidelines and initiatives of the EU and NATO and to support each other with their experiences in developing a national cybersecurity legislation and organisational structure. The most important goal of the platform is to gain more defence and resiliency in case of cyberattacks through this regional cooperation.

The idea of setting up this regional platform can be originated from the historical foundations of the Visegrád countries, which are resting on a cooperative approach since 1991. The Visegrád cooperation is based on the main common aims of the countries concerned like geographical relations, historical traditions, the Euro-Atlantic security system and the accession to the Euro-Atlantic organisations.

20 years later, when the CECSP cooperation was created, the original aims of the Visegrád cooperation was already achieved, but the cooperation was still preserved, to support each other in development and to be able to assert their interest in the international communities. Therefore, the original political Visegrád cooperation has been supplemented with independently operating thematic cooperation like the CEDC and CECSP.

The Central European cybersecurity cooperation is a comprehensive approach to cybersecurity issues, covering major levels of cybersecurity (strategic–operative, government–military, national–international). Accordingly, representatives of the platform include the ministries responsible for cybersecurity, military and national CSIRTs and authorities responsible for information security. In addition, the European Network and Information Security Agency (ENISA) has an observer position in the platform to support the aims and work of the platform with its international experience.[12]

In CECSP, the most important strategic aim of the members is to be more successful in international, community (EU) or allied (NATO) lobbying and to be able to represent a regionally discussed and agreed single position. As a result, Member States will have an opportunity to better reach out the consideration and validation of their positions and proposals on community or allied level. This also can be an important element of cyber diplomacy, to be able to assert our position by getting support from our regional partners. Such cooperation has been observed over the past years during the negotiation of cybersecurity regulations within the European Union (such as the NIS Directive or the EU Cybersecurity Act).

After the establishment of a common, European level international regulation (for example, the adoption of the NIS Directive), the support function of the platform is still important for all of the members, as it can also provide a podium

[12] European Union Agency for Network and Information Security: Meeting of the Central European Cyber Security Platform 2014. *ENISA News,* 10 April 2014.

for discussing legal and technical questions arising during the implementation and evaluating cooperation mechanisms.

Another objective of this cooperation at the strategic level is to create a platform between the countries to support cooperation and share experience in R&D projects, but in practice, there was no visible cooperation or even information sharing within (or with the support of) the platform about their experiences in R&D projects. Probably the regulatory questions were bigger priority or R&D is still such a sensitive topic that it is more important than information sharing and cooperation.

At the beginning, the establishment of cooperation on the operational level was also a huge priority, which is realised in the CERTs/CSIRTs cooperation. As it was seen in the strategies, the objective of most countries was to set up different CSIRTs or to develop the existing ones; information sharing and learning from the experiences of others are essential for the CSIRTs. Just like in other CSIRT communities, members share their experiences, report lessons learnt of major successful or failed attacks and good practices to community members, and make their collaboration more effective by organising cybersecurity exercises in order to develop the skills and preparedness of IT security professionals for current cybersecurity challenges and attacks.

At the beginning, the most important elements on the agenda of the Platform was the CSIRT cooperation (and practice the possible cooperation forms by cyber exercises) and to present and explain to each other their regulatory and organisational framework.

The Operational Model of the CECSP

In 2013, during the establishment of the Platform, the main goal was to build trust, to define a cooperation framework and its rules. After all, there was a need to develop a work program also for the platform.

According to the defined rules, the Platform has at least one strategic and operational meeting each year. The members decided to set up a presidency model, where the presidency is responsible for the management of the platform and the organisation of the meetings. Member States fill the presidency in a rotating system for one year (in alphabetical order). Hungary acted as chairman of the platform in 2015, and in 2020 also Hungary had the chairman position and responsibility.

During the first Hungarian platform presidency in 2015, there was a strategic decision-makers working group meeting and an operational level meeting in Budapest.

Unfortunately, the official work programs of the CECSP presidencies are not publicly available, but we could identify the main aims and most important tasks of the presidency periods thanks to the published Presidency summaries after the events, and to the references to the CECSP's aims and activities in the V4 presidency programs.

In the first few years, the platform organised various cybersecurity exercises for its members yearly, despite the fact that all participating national CERTs in the platform are taking part in EU and NATO exercises. Involving cybersecurity professionals in red and blue teaming exercise can also provide an opportunity to test and discuss the experiences gained in the allied and community exercises.

Until now, Hungary has organised two exercises for the members of the platform. The first one was held on 23 June 2014, right after the establishment of CECSP.[13] The second one was a decision-making and procedural exercise (Table Top Exercise, TTX) in 2015, during the Hungarian presidency period of the platform. The latest exercise took place in May 2017 in Brno, the Czech Republic. It was developed by the Masaryk University and was held in a special environment. This exercise did not focus on cooperation, but on testing and developing the technical skills of participating players.[14] In 2018, no regional exercise took place, as all countries participated at the ENISA's Cyber Europe 2018 cyber crisis exercise event.

Cybersecurity on the Political Level in V4 Cooperation

As it was mentioned and explained before, CECSP is independent from the Institutional Visegrád 4 cooperation and from the Central European Defence Cooperation (CEDC) either, but it could not have taken place without the political support of the governments of the concerned countries. As soon as the political leaders realised the potential impact of cyberattacks, the need of cyber defence on regional level has appeared in the presidency programs (with respect to the

[13] Ádám Draveczki-Ury: Szoros együttműködés a kibertérben. *Honvedelem.hu,* 27 June 2014.

[14] National Cyber Security Center (NCKB): *National Cyber Security Centre Held Exercise for CECSP Partners.* 24 May 2017.

CECSP work program itself) and has evolved parallelly with the NATO–EU objectives.

Naturally, the higher politically represented V4 cooperation has influence and/or refer to the CECSP aims and work program; therefore, it is important to collect and see the cyber-related goals of each V4 presidency from 2012, where this issue was first mentioned.

2012–2013 Polish Presidency

Cybersecurity was first mentioned in the Visegrád 4 work program in a military context:

> "There will be a need for V4 consultations on NATO–Russian relations, a V4 common position on Missile Defence and on the Russian response, on NATO cooperation with Ukraine and Georgia, consultations on CFE and force deployment in the region, consultations, in the broader format of V4+ Baltic states + Romania and Bulgaria, on common security issues, and with regard to cyber security and energy security."[15]

2013–2014 Hungarian Presidency

In this year, cybersecurity got a higher focus because of the establishment of the CECSP, and there was already technical meetings as well, led by the Czech Republic.[16] The V4 members described their goals on political level as follows:

> "– Emphasizing the importance of cyber security awareness and strengthening dialogue and cooperation at policy and operational level in the field of cyber defense;
> – Promoting efforts to make information exchange and knowledge transfer (lessons learned and best practices) more efficient in the field of cyber and information security.
> – Exchange of knowledge and practical expertise countering cybercrime with Western Balkan countries."

The military approach can also be found in this presidency program, as well as cybercrime and cyber diplomacy. The "concrete proposals for discussion" of the

[15] Ministry of Foreign Affairs of the Republic of Poland: Programme of the Polish Presidency of the Visegrad Group. *International Visegrad Fund,* 1 July 2012.

[16] CSIRT.CZ: *Zástupci CSIRT.CZ se zúčastnili setkání platformy CECSP.* 28 December 2013.

V4 countries “include the setting up of a long-term cyber security cooperation mechanism” in the context of security policy related to NATO and the Common Security and Defence Policy of the European Union. They also “endeavour to strengthen the V4–B3 cooperation, particularly in the fields of […] cyber security” and promote further cooperation with the Western Balkan countries “on judicial cooperation in criminal matters and fight against corruption, and fight against cybercrime”.[17]

2014–2015 Slovak Presidency

Information and cybersecurity got a separate chapter in this presidency program and became one of the major issues. “The primary objective is to increase the immunity of information systems in the V4 countries against cyber-attacks and to decrease computer-based crime.” To reach this goal, the Slovak presidency focused on the following topics:

> “– Streamlining management of information/cyber security, security risk management;
> – Protecting human rights and fundamental freedoms in connection with the use of information and communication infrastructure (including the Internet);
> – Increasing awareness and competencies, education in the area of information/cyber security;
> – Cooperation at international level in the area of information/cyber security (exchanging skills, experience and sharing information);
> – Completing mutual consultations in order to harmonize the approaches taken by V4 countries and considering mutual support when adopting decisions and their subsequent implementation within international organizations (EU, NATO, UN and others);
> – Supporting an improvement in the standing of the Central European Cyber Security Platform;
> – Creating a safe environment (prevention, response to security incidents, the scope of specialized CSIRT/CERT-type teams, for example the implementation of joint simulation exercises on critical information infrastructure protection, creating a secure communication channel to share information on current threats and on-going large-scale security incidents, linking of early warning and information sharing in the V4.”[18]

[17] Ministry of Foreign Affairs and Trade of Hungary: Hungarian Presidency in the Visegrad Group (2013–2014). *International Visegrad Group,* 1 July 2013.

[18] Ministry of Foreign and European Affairs of the Slovak Republic: Programme of the Slovak Presidency of the Visegrad Group, July 2014 – June 2015. *International Visegrad Group,* 1 July 2014.

This program has defined the scope of CECSP cooperation, and the platform is still working according to the above described principles. In this year, cyber did not appear in any other relation, except the defence and security policy part, where it was treated as a general security risk.

2015–2016 Czech Presidency

The Czech Presidency placed cybersecurity to the operational level. As CECSP's operational capability has been proven, this issue disappeared from the list of strategic questions. The Presidency Program has the following statement:

> "Cybersecurity is also a prospective topic for the Visegrád cooperation. The CZ V4 PRES will push to deepen and increase the efficiency of cooperation within the Central European Cyber Security Platform (CECSP). This will particularly include harmonising the positions of the V4 countries on fundamental topics of cyber security, including their positions within international organisations, organising expert workshops and introducing standards and secured channels as part of communication among the CECSP states. The V4 will also continue in the practice of cooperation among specialised police units and national 'centres of excellence' focused on research in the area of cybernetic crime."[19]

The Czech National Security Authority got the task to facilitate the operational level cooperation. For this, their planned activities also were specified in the program:

> "– At the strategic level, the CZ V4 PRES will seek progress in harmonising the approach of individual states and their positions and opinions on major cyber security issues within international organisations, forums and discussions. This includes primarily the legislation being negotiated in the working bodies of the Council of the EU and European Commission and documents negotiated under the OSCE and International Telecommunication Union;
> – At the operational level among top CERT sites, we want to organise workshops on selected topics (e.g. intrusion detection and honeypots, penetration testing, etc.);
> – The CZ V4 PRES is committed to implementing standards and secure channels in communications among CECSP states."[20]

[19] Ministry of Foreign Affairs of the Czech Republic: Programme for the Czech Presidency of the Visegrad Group 2015–2016. *International Visegrad Fund,* 1 July 2015. 12–29.

[20] Ibid.

2016–2017 Polish Presidency

Following the approach of the previous year, cybersecurity remained on the technical level and highlights the importance of CECSP. This area is summarised only in one paragraph:

> "Cyber-security: cooperation to enhance the protection against cyber threats inter alia by means of CSIRT cooperation and the Central European Cyber Security Platform (CECSP); building permanent relations between the CECSP and the V4. Furthermore, encouraging cooperation between special Police units and national 'centres of excellence' that focus on conducting research in the field of cyber-crime."[21]

Cybersecurity also disappeared from the defence policy and was only mentioned once under the police cooperation part, in relation with cybercrime. Probably the reason behind this reduced priority can be found in the European legislation. As, in this period, the NIS Directive was adopted and required a pan-European approach for cyber defence. The need for a regional cooperation has seemingly decreased.

2017–2018 Hungarian Presidency

2017 was a turning point in the era of cybersecurity. There were two state sponsored malware campaigns (WannaCry and NotPetya) that caused global chaos, meanwhile more and more details had been revealed on the effects of cyberattacks during the U.S. presidential election. The Hungarian Presidency Program clearly reflects to these threats and cyber defence got a higher focus than in the previous year.

First of all, due to hybrid threats, cybersecurity is mentioned in a military context again:

> "Defence policy cooperation in the V4 + Ukraine and V4 + Moldova formats, focusing on examining possibilities for joint work on defence sector reform, sharing experience on cyber defence and hybrid war, resilience and a potential involvement in the V4 EU Battlegroup (in the case of Ukraine)."

[21] Ministry of Foreign Affairs of the Republic of Poland: Programme of the Polish Presidency of the Visegrad Group 2016–2017. *International Visegrad Fund,* 1 July 2016. 14.

This is emphasised with a planned Cyber Workshop between the V4 countries and the United States.

On the other hand, the operational cooperation is described in more details:

> "In the field of cyber security, the Presidency's goal is to strengthen the resilience of critical infrastructure, especially with the aim of revealing and averting risks and attacks coming from the cyberspace. The Hungarian Presidency will carry on the cooperation between cyber security organisations and network security centres of V4 countries, for which information-sharing on incidents is indispensable. In cooperation with the rotating Chair of the Central European Cyber Security Platform, the Hungarian Presidency will organise expert meetings and joint exercises and trainings related to incident management. The Presidency also plans to hold consultations aiming to formulate joint V4 positions on current topics of the EU's agenda, in particular on the implementation of the Directive on Security of Network and Information Systems (NIS Directive), and the revision of the Cybersecurity Strategy of the EU."[22]

2018–2019 Slovak Presidency

This Presidency Program also deals with cybersecurity, but it is not as ambitious as it was in the previous year. It focuses on cybercrime and the usage of cryptocurrencies:

> "Digital evolution and the development of cyber space bring an increasing number of cyberattacks, which, in some EU Member States, even exceed the number of standard crimes. Therefore, within the Presidency of the V4, we shall focus on the strengthening and improvement of cooperation in the fight against cybercrime connected with the misuse of crypto currencies, especially bitcoin."

Then it turns to CECSP and highlights the success of the Slovak Presidency of this forum in 2017:

> "With regard to CECSP cooperation, during the Slovak Presidency in 2017 the member countries started to coordinate their activities, stances, and positions even on the EU level. This initiative did not go unnoticed by other members of the EU. For example, as a result France joined in on the coordination of CECSP activities in matters of the cybersecurity of the European Union."[23]

[22] Ministry of Foreign Affairs and Trade of Hungary: Hungarian Presidency 2017–2018 of the Visegrad Group. *International Visegrad Group,* 1 July 2017. 15–16.

[23] Ministry of Foreign and European Affairs of the Slovak Republic: Dynamic Visegrad for Europe, Slovak Presidency 2018–2019 of the Visegrad Group. *International Visegrad Group,* 1 July 2018. 18.

2019–2020 Czech Presidency

This presidency program is also not too ambitious regarding cybersecurity as it is nearly just mentioned in the detailed presidency program.

The Czech presidency program has 3 main priority areas (mentioned as a 3R), and cybersecurity related topics are covered in the second one. This area is the area of the Revolutionary technologies, where presidency aims to deal with

> "innovative economy and its social impacts: CZV4PRES will concentrate on support for research, development and innovation, innovative ecosystem, Digital Single Market, artificial intelligence but also on education and adaptability of people to the related changes in the labour market."[24]

As part of the detailed presidency program, the Czech presidency mentions cybersecurity-related topics also as part of the security policy

> "to include European defence initiatives and the development of the civilian component of the Common Security and Defence Policy. The objective is to enhance security and defence cooperation especially in collective defence, military mobility, cyber security, hybrid threats, terrorism, strategic communication capabilities, and regarding challenges emanating from the South."

Cybercrime and critical infrastructure protection is also mentioned in the presidency program, with the aim to

> "promote closer V4 exchange of experience and cooperation on cybercrime, especially between national cybercrime contact points and law enforcement authorities (public prosecutors and the police). The focus should be on the protection of critical information infrastructure and important information systems."[25]

Supporting these goals, only one event, a conference has been organised (and planned in the work program) in November 2019, by the Czech Republic Police about the current trends in cybercrime and cybersecurity.

[24] Ministry of Foreign Affairs of the Czech Republic: *The Czech Republic Holds the Presidency of the Visegrad Group from 1 July 2019 to 30 June 2020.* 25 June 2019.

[25] Ministry of Foreign Affairs of the Czech Republic: Programme for the Czech Presidency of the Visegrad Group 2019–2020. *Visegrad Group,* 06 September 2019.

In this presidency program, the CECSP cooperation or the operational cybersecurity cooperation has not been mentioned, furthermore the work program defines task and cooperation only for the police and for the Ministries of Foreign Affairs.

Probably the reason of the disappearance of the CECSP and operational cyber policy from the V4 presidency programs could be found in the developed EU cyber policy. For this time, this cooperation forms were established in EU level by the NIS Directive and Cyber Act, and the possible future work must be raised within the parties in the future.

2020–2021 Polish Presidency

The pandemic situation and its consequences have a huge effect on the presidency program of 2020–2021; therefore, the Polish presidency will mainly focus on the Covid-related issues, but cybersecurity can also be found in its agenda, as an important issue in a pandemic situation like the Covid-19.

The Polish residency is planning to discuss its initiatives in the cybersecurity area:

> "Signing a joint declaration on mutual cooperation in cyber security, to serve as a roadmap for V4 activities – main activity areas include:
> – increasing the capability for reacting to incidents by, among others, developing the management of cross-border incidents in combination with consultations, as well as conducting international exercises to improve adaptation in taxonomy, collection and analysis of digital evidence and collaboration in prosecuting cyber criminals;
> – building common situational awareness in cyber space, especially by exchanging information on cyber threats in real time between national level CSIRT teams;
> – developing new methods and tools to test, assess and certify ICT products, processes and services (as part of the Cyber Security Act);
> – developing a new generation of cryptographic algorithms resistant to quantum computing;
> – improving multilateral collaboration and national capabilities in cyber security, among others in the R&D area."[26]

Furthermore, the Polish presidency is planning to consult within the CECSP platform about the other possible topics (like cross-border incident handling;

[26] Ministry of Foreign Affairs of the Republic of Poland: Presidency Programme of Polish Presidency of the Visegrad Group 2020–2021. *International Visegrad Fund,* 1 July 2020.

situational awareness; R&D, supply chain security; digital evidence and international law applicable to cyberspace operations) that can be involved within the regional cooperation.

Efficiency, Benefits and Future of CECSP Cooperation

As we saw before, the participating countries have common objectives, basic regulations and an organisational system for the operation of the Central European Platform. Since the establishment of the cooperation, mainly operational and strategic discussions and cybersecurity exercises were on their agenda. The essential and basic requirement for the effective functioning of the cooperation is to build trust between the parties involved in the agreement. We can say that the countries participating in the platform are familiar with the legal and organisational specialties of each other in detail and had the opportunity to build up trust and to understand other parties. This completely meets our definition of cyber diplomacy.

As a result, they had opportunity for detailed technical consultations, discussions and could identify additional actors and areas of expertise for the further development and deepening of the cooperation.

After examining the work programs of the platform, we could see that this cooperation mainly stayed at the strategic cooperation level, where political (EU, NATO and national) legal and diplomatic questions have been discussed. We also saw some intention for a deeper cooperation by involving CSIRTs in this cooperation, but it stayed on a higher level by sharing best practices, introducing themselves and their main knowledge (but not in detail). Cyber exercises do not mean real cooperation either; it is just practicing their ability and cooperation model. IT helps to build trust, but it is still far from real life technical cooperation (in case of an incident, or a project etc.).

As it was mentioned above, the NIS Directive, adopted in 2016, is the first European regulation to provide mandatory legislative and technical (CSIRT) cooperation and defines minimum requirements in the national regulation for the Member States. Accordingly, the CECSP Member States had to review their national cybersecurity strategy, in line with NIS requirements, as well as their national legislation for the core services sectors and the sectors providing digital services. As a result, the CECSP member states have the same national strategy, national regulations and organisational structure and are set up on the same basis.

Thanks to the directive, collaboration and information sharing between CSIRTs is implemented through binding rules, in case of incident reporting and cross-border incident management as well. The technical training and testing area are also covered by the European Union regulations, as there are mandatory exercises, like the Cyber Europe exercise in every two years, and the exercises of the CSIRTs Network.

The question may arise that after these rules and cooperation mechanisms established by the NIS Directive, what can be the role of the CECSP regional cooperation if all its countries are members of the EU and must apply the EU level cooperation.

It is undeniable that the strategic and technical cooperation elements of the Platform are covered by the new EU rules, and the V4 presidency programs and the decrease of the operation of the CECSP meetings also pointing to the direction that CECSP has been replaced by the EU level cooperation.

On the other hand, most of the members still mention the need and the importance of the regional cooperation in their new cybersecurity strategies, so probably they do not plan to terminate the platform, but they have their main focus on other international cooperation.

Maybe it would be important to find new aims and cooperation areas for the platform, as the active cooperation and effectiveness of the platform decreased since the implementation of the NIS Directive.

2020 seemed to be an interesting and promising year from several perspectives: first of all, Hungary held the presidency of the platform again, and that could have been a huge opportunity to discuss and refresh the aims of the platform. Secondly, in 2020 the European Commission assessed the implementation and effectiveness of the NIS Directive and defined the suggestion on how to redraft the directive, and it could also have been a good opportunity to draft a common position and suggestion for the Commission about the NIS Directive. Unfortunately, in that year the Covid crisis has overwritten every kind of plans, events and discussions, and maybe it has a negative effect on such regional policy-related discussions as well. Unfortunately, we do not have any publicly available information or report about the programme or results of the 2020 programme of the platform, but probably the programme has been minimised to discuss the Covid-related issues, and the NIS-related review, and probably the events must be delayed or changed to remote events, which also reduces the effectiveness of such discussions.

But there are several promising issues that could be discussed, and handled within the platform, as they are still not regulated by the EU, and it could add value to the regional work. The participants can review the existing CECSP cooperation and involve more professionals from other areas, and extend the cooperation with some other, more specialised areas (such as research and development, education, awareness raising, law, professional training, common EU research applications, cross-sectoral issues, etc.). The support of actual CECSP parties (ministries, authorities and CSIRTs) for the new areas of the regional cooperation could help the new partners in trust- and confidence-building and could be a good basis to start a valuable, deep and daily cooperation.

Finally, it should be emphasised that the platform still gives a good opportunity for its members to develop a stronger common position on international level and can be a forum to discuss ideas, questions and experiences at the transposition stage as they have already done regarding the NIS Directive and the Cybersecurity Act.

As we can see, cyber diplomacy is an important and integral element of the regional cooperation of the Visegrád countries, were they have an opportunity to discuss legal and organisational (and maybe technical) questions, as well as questions of cooperation, to develop together different cyber exercises to have an opportunity to establish a common position to be able to validate their position in other international forums.

References

Berzsenyi, Dániel: Kiberbiztonsági analógiák és eltérések. A Közép-európai Kiberbiztonsági Platform részes országai által kiadott kiberbiztonsági stratégiák összehasonlító elemzése. *Nemzet és Biztonság,* 7, no. 6 (2014). 110–136.

CSIRT.CZ: *Zástupci CSIRT.CZ se zúčastnili setkání platformy CECSP.* 28 December 2013. Online: www.csirt.cz/page/1836/zastupci-csirt.cz-sezucastnili-setkani-platformy-cecsp/

CSIRT.SK: *Third meeting of CECSP: Tretie rokovanie Stredoeurópskej platform kybernetickej bezpečnosti.* 11 April 2014. Online: www.csirt.gov.sk/aktualne-7d7.html?id=69

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union. Online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L1148

Draveczki-Ury, Ádám: Szoros együttműködés a kibertérben. Honvedelem.hu, 27 June 2014. Online: https://honvedelem.hu/cikk/szoros-egyuttmukodes-a-kiberterben/

European Union Agency for Network and Information Security: Meeting of the Central European Cyber Security Platform 2014. *ENISA News,* 10 April 2014. Online: www.enisa.europa.eu/news/enisa-news/central-european-cyber-security-platform-2014

Federal Ministry for Digital and Economic Affairs: Central European Cyber Security Platform. *Digitales Österreich,* 11 April 2014. Online: www.digitales.oesterreich.gv.at/-/central-europeancyber-security-platform

Government of the Czech Republic: National Cyber Security Strategy of the Czech Republic for the Period from 2015 to 2020. *ENISA,* 16 January 2015. Online: www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf

Government of Hungary: Government Decision No. 1838/2018 (28 December 2018) on Hungary's Strategy for Network and Information Security.

Government of Hungary: Government Decision No. 1139/2013 (21 March) on the National Cyber Security Strategy of Hungary. *ENISA,* 21 March 2013. Online: www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/HU_NCSS.pdf

Government of Poland: National Framework of Cybersecurity Policy of the Republic of Poland. *ENISA,* 30 November 2017. Online: www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/govermental-program-for-protection-of-cyberspace-for-the-years-2011-2016-2013

Government of the Slovak Republic: Cyber Security Concept of the Slovak Republic. *ENISA,* 01 June 2015. Online: www.enisa.europa.eu/topics/national-cyber-securitystrategies/ncss-map/cyber-security-concept-of-the-slovak-republic-1

Kovács, Lászó: *Kiberbiztonság és -stratégia.* Budapest, Dialóg Campus, 2018.

Ministry of Foreign and European Affairs of the Slovak Republic: Programme of the Slovak Presidency of the Visegrad Group, July 2014 – June 2015. *International Visegrad Group,* 1 July 2014. Online: www.visegradgroup.eu/documents/presidencyprograms/sk-v4-pres-program-2014

Ministry of Foreign and European Affairs of the Slovak Republic: Dynamic Visegrad for Europe, Slovak Presidency 2018–2019 of the Visegrad Group. *International Visegrad Group,* 1 July 2018. Online: www.visegradgroup.eu/documents/presidency-programs/slovak-v4-presidency-en

Ministry of Foreign Affairs and Trade of Hungary: Hungarian Presidency in the Visegrad Group (2013–2014). *International Visegrad Group,* 1 July 2013. Online: www.visegradgroup.eu/documents/presidency-programs/hu-v4-presidency-2013

Ministry of Foreign Affairs and Trade of Hungary: Hungarian Presidency 2017–2018 of the Visegrad Group. *International Visegrad Group,* 1 July 2017. Online: www.visegradgroup.eu/documents/presidency-programs/hungarian-v4-presidency

Ministry of Foreign Affairs of the Czech Republic: Programme for the Czech Presidency of the Visegrad Group 2015–2016. *International Visegrad Fund,* 1 July 2015. Online: www.visegradgroup.eu/documents/presidency-programs/cz-v4-pres-2015-2016

Ministry of Foreign Affairs of the Czech Republic: *The Czech Republic Holds the Presidency of the Visegrad Group from 1 July 2019 to 30 June 2020.* 25 June 2019. Online: www.mzv.cz/jnp/en/foreign_relations/visegrad_group/index.html

Ministry of Foreign Affairs of the Czech Republic: Programme for the Czech Presidency of the Visegrad Group 2019–2020. *Visegrad Group,* 06 September 2019. Online: www.mzv.cz/file/3626458/Programme_CZ_V4_PRES_2019_2020_A.pdf

Ministry of Foreign Affairs of the Republic of Poland: Programme of the Polish Presidency of the Visegrad Group. *International Visegrad Fund,* 1 July 2012. Online: www.visegradgroup.eu/documents/presidency-programs/programme-of-the-polish

Ministry of Foreign Affairs of the Republic of Poland: Programme of the Polish Presidency of the Visegrad Group 2016–2017. *International Visegrad Fund,* 1 July 2016. Online: www.visegradgroup.eu/documents/presidency-programs/pl-v4-pres-2016-17

Ministry of Foreign Affairs of the Republic of Poland: Presidency Programme of the Polish Presidency of the Visegrad Group 2020–2021. *International Visegrad Fund,* 1 July 2020. Online: www.visegradgroup.eu/documents/presidency-programs/2020-2021-polish

National Cyber Security Center (NCKB): *Central European Cyber Security Platform 2014.* Online: www.govcert.cz/cs/informacni-servis/akce-udalosti/2140-central-european-cyber-security-platform-2014/

National Cyber Security Center (NCKB): *National Cyber Security Centre Held Exercise for CECSP Partners.* 24 May 2017. Online: www.govcert.cz/en/info/events/2532-national-cyber-security-centre-held-exercise-for-cecsp-partners/

National Cyber Security Center (NCKB): National Cyber Security Strategy of the Czech Republic for the Period from 2021 to 2025. *NUKIB,* 18 March 2021. Online: www.nukib.cz/download/publications_en/strategy_action_plan/NSCS_2021_2025_ENG.pdfNational

Security Authority (NBU): The National Cybersecurity Strategy 2021–2025. *NBU,* 07 January 2021. Online: www.nbu.gov.sk/wp-content/uploads/cyber-security/National_cybersecurity_strategy_2021.pdf

Nemzeti Kibervédelmi Intézet: Megrendezésre került a Közép-európai Kiberbiztonsági Platform (CECSP) konferencia. *NKI,* 21 December 2013. Online: https://nki.gov.hu/figyelmeztetesek/archivum/megrendezesre-kerult-a-kozep-europai-kiberbiztonsagi-platform-cecsp-konferencia/

Németh, Bence: *Outside NATO and the EU. Sub-Regional Defence Co-Operation in Europe.* London, King's College, 2017. Online: https://kclpure.kcl.ac.uk/portal/files/80807208/2017_Nemeth_Bence_1212105_ethesis.pdf

Republic of Austria: *Austrian Cyber Security Strategy.* 10 March 2013. Online: www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/AT_NCSS.pdf

Republic of Poland: Uchwała Nr 125, Rady Ministrów w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024. 12 October 2019. Online: http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WMP20190001037/O/M20191037.pdf

Tikos, Anita – Csaba Krasznay: *Cybersecurity in the V4 Countries – A Cross-border Case Study.* Central and Eastern European e|Dem and e|Gov Days 2019. 163–174. Online: https://doi.org/10.24989/ocg.v335.13