CYBERSECURITY IN THE V4 COUNTRIES – A CROSS-BORDER CASE STUDY

Anita Tikos[1] and Csaba Krasznay[2]

DOI: 10.24989/ocg.v335.13

Abstract
Information sharing is one of the major issues in cybersecurity nowadays. Although it is essential for all players in the cyberspace to get relevant information on the latest threats but giving such threat intelligence for others is not as easy as it seems. Obviously, there are national rules and regulations that make this difficult, but the lack of trust between the different entities is also a challenge, especially when such data should cross the borders. The Visegrad 4 countries started an exemplary cooperation under the name of Central European Cyber Security Platform or CECSP a few years ago that can serve as a case study for similar multilateral initiatives. In this paper, we present the history of this cooperation, the actual achievements and difficulties in practice. Besides the literature review, we also highlight our thoughts of from the practitioners' approach as we are participating in the daily operative collaboration. Based on the findings we propose some steps how these countries should go beyond the actual results.

1. Introduction

Today, thanks to the rapid development of information technology and the expansion of digitization, cyberspace becomes a significant part of our life, as electronic public services, digital economy and networked society play an important role both in our work and in our general activities. The importance of digital infrastructures and services in public, financial, educational and economic processes is indisputable. Meanwhile, threats from cyberspace are dynamically growing in parallel with the development of digital infrastructures and services, therefore the security-related improvement of cyber ecosystem has become an increasingly important issue.

In the last decade cybersecurity has appeared as a key challenge for all countries and organizations, resulting the establishment of organizations or divisions that are responsible for the creation and maintenance of information security (e.g. authorities, CSIRTs[3], Security Operation Centers, cyber defense agencies or centers of excellence, etc.). Due to the possible cross-border nature of threats and incidents, it became relatively clear at an early stage that in addition to the above-mentioned IT security organizations, cooperation through various international forums and mechanisms is also needed.

[1] University of Óbuda Doctoral School on Safety and Security Sciences, H-1081 Budapest, Népszínház u. 8., anita.tikos@gmail.com, www.uni-obuda.hu
[2] National University of Public Service Institute of E-government, H-1083 Budapest, Üllői út 82., krasznay.csaba@uni-nke.hu, www.uni-nke.hu
[3] Computer Security Incident Response Team

First, the communities of incident management centers (CERT[4]/CSIRT) have been set up, followed by the development of common strategic objectives and cooperation. By now, the main international organizations (NATO, EU, ITU, OSCE) all put cybersecurity on their agenda. Currently, many bilateral, international, sectoral, strategic and operational cooperation works worldwide.

This wide list of cooperation was augmented in 2013, as the Czech Republic and Austria has initiated a regional cooperation by the name of Central European Cyber Security Platform or CECSP. The regional agreement has created strategic and operational cooperation between the four Visegrád countries (Czech Republic, Hungary, Poland, Slovakia) and Austria. CECSP is a natural next step of the Central European Defense Co-operation (CEDC), established in 2011, but it is not part of the latter one. Besides the five countries, Slovenia is also one of the founding member states of CEDC, that aims to facilitate the military-focused collaboration. There is only one similar, regional defense platform in Europe, NORDEFCO, founded by the Nordic countries, but it doesn't have a specific, cybersecurity-oriented agreement. [20]

The question may arise, considering that CECSP countries are participating in several already existing organizations, that what new role can be played by CECSP, what added value can it create in the cooperation with other operational and strategic levels. To answer this question, an overview is needed on the platform's participants and their goals and activities in the cyberspace.

2. CECSP countries' cyber security structure

Countries that are members of the platform participate in the activities of the major international communities without exception, and because of the fact that cyber security regulations of these communities are developing into the same direction, CECSP countries have essentially similar legal and organizational structures. [1] It is important to emphasize that until 2016, when Directive on security of network and information systems (NIS Directive) was adopted, only guidelines and strategic objectives from international organizations and national experiences (best practices) have shown examples internationally, therefore the countries' preparedness and organizational system was different. [5]

It is worth comparing the cybersecurity preparedness and system of the countries that are members of the platform on the basis of their national strategy and organization system. The detailed strategic and organizational analysis is not part of the present study, only the highlighting of the main similarities and differences is our aim by drawing up a comprehensive picture.

The first national cyber security strategies were established at about the same time by the CECSP countries. 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 [8] [21] [22] [23] [24]. Of course, over the years most of them have reviewed their strategy, as Slovakia and the Czech Republic formulated a new strategy for the period 2015-2020, meanwhile Poland published its own in 2017. Hungary also extended its own cybersecurity strategy with a sectoral strategy required by the NIS Directive in 2018. In their case, the legal and organizational review is made based on the latest edition.

[4] Computer Emergency Response Team

We can say that the national strategies 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. The strategies under consideration vary from the legislative perspective. Some of the strategies aims the creation or the update of a comprehensive information security regulation (for 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 cyber security organizations, it should be highlighted that all evaluated strategies identify the governmental and/or national incident management center (GovCERT / national CERT), the regulatory body with rights and responsibilities and the organization or ministry responsible for coordination and for decision-making. [9]

There is a discrepancy between the regulation of areas outside the government, the regulation of critical infrastructures and the organizational coverage. In case of some strategies, the development of regulations and the creation of specialized organizations 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 strategies deal with question of non-governmental, sectoral CERTs and the establishment military CERTs. The countries have a same approach in terms of the need for the creation of special sectoral CERTs. In Austria, there are many commercial CERTs are operating and has a military CERT (MilCERT), whereas in Hungary and the Czech Republic one of the objectives is the establishment of a sectoral CERT.

The strategies cannot be used to draw a conclusion on the similarity or differences of the organizational structures, as a number of organizational development and transformation took place in the Member States due to the adoption of the strategies, such as the creation of commercial CERTs or the formation of military CERTs. For example, in Hungary the Defense Sector Electronic Information Security Incident Management Center (MilCERT) was established in March 1, 2016.

3. Objectives and operation of Central European Cyber Security Platform

In accordance with the fundamental objectives of the CECSP countries, the main aims of the close regional cooperation are to work together in accordance with the policies, initiatives of EU and NATO and to help each other with their experiences in developing a national cybersecurity legislation and organizational structure. The most important goal of the platform is to gain more defense and resiliency in case of cyberattacks through this regional cooperation. The peculiarity of this platform is that the historical foundations of the Visegrád countries are resting on a cooperative approach since 1991 towards European integration. CECSP 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 or authorities responsible for information security. In addition, the European Network and Information Security Agency (ENISA), with its international experience, assists and supports the work of the platform as an observer. [7]

In CECSP, the aim of the highest-level cooperation 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. Such co-operation and reconciliation has been observed over the past years when negotiating 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 maintained, since it can also provide a podium for discussing legal and technical issues 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.

We can also mention the establishment of cooperation on the operational level as a priority goal, which is realized in the CERTs / CSIRTs cooperation. 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 organizing cybersecurity exercises in order to develop the skills and preparedness of IT security professionals for current cybersecurity challenges and attacks.

In 2013, when the platform was created, the main goal was to build trust, to define a cooperation framework and its rules and to develop a work program. Each year, the platform has at least one strategic and operational meeting. The presidency is responsible for the management of the platform and the organization of the meetings. Member States fill the presidency in a rotating system for one year (in alphabetical order). Hungary in 2015 acted as chairman of the platform. In this year, there was a strategic-decision-makers working group meeting and an operational level meeting in Budapest.

Each year, the platform organizes various cyber security exercises for its members, despite all participating national CERTs in the platform are taking part in EU and NATO exercises without exception. In addition to practice the skills of professionals involved in red and blue teaming, such events can also provide an opportunity to test and discuss the experiences gained in the allied and community exercises and conclude them in a narrower community.

So far, Hungary has organized two exercises for the members of the platform. The first one was held in 23 June 2014, right after the establishment of CECSP. [6] The second one was a decision-making and procedural exercise (Table Top Exercise, TTX) in 2015, when Hungary was the president 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 didn't focus on cooperation, but on testing and developing the technical skills of participating players. [18] In 2018, there wasn't any regional exercise, as all countries participated in ENISA's Cyber Europe 2018 cyber crisis exercise event.

4. Cybersecurity on the political level in V4 cooperation

As we mentioned before, CECSP is independent from the institutional V4 cooperation or from the Central European Defense Co-operation (CEDC), but it couldn't come alive without the political support of the governments of the affected countries. As soon as the political leaders realized the potential impact of cyberattacks, the need of cyberdefense on regional level has appeared in the presidency programs and has evolved parallelly with the NATO/EU objectives.

CEDC, CECSP and the V4 are all independent cooperation, that has their own work programs, priorities. These cooperation mechanisms support and respect each other, therefore if they have similar priority or aim in their agenda, they make it in a joint effort (for example a joint conference, workshop of the V4 and the CECSP presidencies). It is important to highlight, that the work program and the meeting agendas of the CECSP are not publicly available, while this is a close cooperation of the governmental and national CSIRTs, authorities, National Cyber Security Agencies, which in some countries (in Hungary and in Slovakia) work within a special service. For this paper, we can use only the official articles and short online reports of the participant organizations as a reference. Therefore, in this part we review the cyber-related goals of each V4 presidency from 2012, where this issue was first mentioned.

4.1. 2012/2013 Polish Presidency

Cybersecurity was first mentioned in this 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]

4.2. 2013/2014 Hungarian Presidency

In this year, cybersecurity got a higher focus due to CECSP, that was led by the Czech Republic in 2013 and Austria in 2014. That was an intensive time, the Member States met for a technical meeting in Prague [2] [19] and on a strategic meeting in Vienna [3] [4] [17]. Meanwhile, on the political level the parties described their goals 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."

We can also identify the military approach, but cybercrime and cyber diplomacy also appeared in this year. V4 countries proposed "discussion include the setting up of a long-term cyber security cooperation mechanism" in the context of security policy and related to NATO and the Common Security and Defence Policy of the European Union. They also "endeavor 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." [12]

4.3. 2014/2015 Slovak Presidency

Information and cyber security 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, Slovakia 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." [11]

As we can see, this program has defined the scope of CECSP cooperation, and the platform is still working based on the above-mentioned principles. In this year, cyber didn't appear in any other relation, except the defense and security policy part, where it was treated as a general security risk.

4.4. 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 Visegrad 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."

The Czech National Security Authority got the task to facilitate the operational level cooperation. Their specific activities 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." [14]

4.5. 2016/2017 Polish Presidency

Following the previous year's approach, cybersecurity remained on the technical level and highlights the importance of CECSP. This area is summarized 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." [16]

Cybersecurity also disappeared from the defense policy and was only mentioned once under the police cooperation part, in relation with cybercrime. We can find the reason of this low priority in the European legislation. In this year, the NIS Directive was adopted and required a pan-European approach for cyber defense. The need for a regional cooperation has seemingly decreased.

4.6. 2017/2018 Hungarian Presidency

2017 is 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 US presidential election. The Hungarian Presidency Program clearly reflects to these threats and cyberdefense 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)". This is emphasized 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), and the revision of the Cybersecurity Strategy of the EU." [13]

4.7. 2018/2019 Slovak Presidency

The actual Presidency Program also deals with cybersecurity, but it's 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."

Than 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." [10]

5. Effectiveness, benefits and future of CECSP cooperation

As it was mentioned before, the work program of the CECSP cooperation, the agenda and the outcome of the meetings are not publicly available, so we can draw our conclusion mainly from the official reports and articles of the participant organizations (CERTs, Cybersecurity Centers and Authorities). Participating countries have common objectives, basic regulations and organizational system for the operation of the Central European Platform. According to the articles, since the establishment of the CECSP cooperation, mainly the basic operational and strategic discussions and annual cyber security exercises can be observed.

For the effective trust building, it is important to know how does the other parties work, what are their organizational and legal structure, moreover, the creation of personal contacts is also essential. We can say that thanks for the first two years of the CECSP cooperation, the countries participating in the platform are familiar with the legal and organizational features of each other in detail and had the opportunity to build up the trust and to understand other parties. Naturally, the platform needed to create cooperation methods to direct the information sharing, CSIRT cooperation, that could be tested, analyzed and further developed by cyber exercises. 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 the cooperation.

It is clearly seen that before 2018, there were different type of cyber exercises within the platform. At the beginning, in 2014 and 2015 there were decision making and procedural exercises (so called table top exercises), where the platform tested and practiced its cooperation methods and rules. The development of the cooperation can be clearly seen in this area, as the type of the platform exercise changed and deepened. In 2016 the Czech National Cyber Security Center held a red team – blue team technical exercise for the CECSP CSIRT partners. During this exercise, the players' technical skills were tested and trained, furthermore, the information sharing amongst them were also tested and trained.

The CECSP platform gave a good opportunity to share our best practices for each other and to gather ideas for further national developments. A good example for this also can be the exercise

held by the National Cyber Security Center of Czech Republic, because the exercise was held within a closed, specially built technical environment, as a so called cyber range. This cyber range was created by a special PPP cooperation of the Government (National Cyber Security Center), a University (Masaryk University) and private companies.

Another important element of the development of cooperation and trust was that the participating countries had the opportunity to jointly face with the international requirements (EU and other international regulation) and cybersecurity challenges (e.g. WannaCry, NotPetya, etc.) in the past years.
As it was mentioned above, the NIS Directive, adopted in 2016, is the first European regulation to provide mandatory legislative and technical (CSIRT) co-operation and defines minimum requirements in national regulation for the Member States. Accordingly, the CECSP Member States had to review their national cyber security 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 nearly the same national strategy, national regulations and organizational structure and are set up on the same basis.

Collaboration and information sharing between CSIRTs is implemented through binding rules, in case of incident reporting and cross-border incident management as well. In the area of cybersecurity exercises, some mandatory events are also required, like Cyber Europe exercise and the exercise of CSIRT Network, etc., therefore the questions of technical trainings and the testing of cooperation arrangements is also covered by the European Union.

The question may arise that besides the rules and cooperation mechanisms established by NIS Directive and Cybersecurity Act what role does the regional cooperation play in the small group of EU members? It is undeniable that the strategic and technical cooperation described in this paper is covered by the new EU rules, but the operational cooperation of the CSIRTs and the strategical cooperation of the authorities can be used and further developed on EU level. The already existing regional cooperation, the built trust, the regional discussions and developments should not be finished, but it could be continued and transposed to other, more specialized areas (such as research and development, education, awareness raising, law enforcement, professional training, common EU research applications, etc.). It is important to see that within the EU, regional cooperation is still an important issue, that should be supported and strengthened, for example in research and development projects, trainings etc. Inclusion of actual CECSP parties (authority and CSIRT) into these new areas of cooperation and confidence-building between the parties can be beneficial and can be a logical next step of the platform.

Finally, it should be emphasized that the platform will still provide a perfect opportunity in the future for countries to develop a stronger common position on international level and can be forum to discuss their ideas, questions and experiences at the transposition stage. We highly propose to pay special attention to the Cybersecurity Act, as this EU legislation is a unique opportunity for the V4 countries' cybersecurity ecosystem.

6. References

[1] BERZSENYI, D., "Kiberbiztonsági analógiák és eltérések. A Közép-európai Kiberbiztonsági Platform részes országai által kiadott kiberbiztonsági stratégiák összehasonlító elemzése" *Nemzet és Biztonság*, 2014/6, pp. 110-136, 2014.

[2] CSIRT.CZ, "Zástupci CSIRT.CZ se zúčastnili setkání platformy CECSP", *CSIRT.CZ*, December 28, 2013. [Online], Available: https://www.csirt.cz/page/1836/zastupci-csirt.cz-se-zucastnili-setkani-platformy-cecsp/ [Accessed: January 22, 2019]

[3] CSIRT SK, "Third meeting of CECSP: Tretie rokovanie Stredoeurópskej platformy kybernetickej bezpečnosti". *CSIRT.SK*, April 11, 2014. [Online], Available: https://www.csirt.gov.sk/aktualne-7d7.html?id=69 [Accessed: January 22, 2019]

[4] Digitales Österreich, "Central European Cyber Security Platform", *Digitales Österreich*, April 11, 2014. [Online], Available: https://www.digitales.oesterreich.gv.at/-/central-european-cyber-security-platform [Accessed: January 22, 2019]

[5] 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

[6] DRAVECZKI-URY, Á., "Szoros együttműködés a kibertérben", *honvedelem.hu*, June 27, 2014. [Online], Available: https://honvedelem.hu/44957 [Accessed: January 22, 2019]

[7] European Union Agency for Network and Information Security, "Meeting of the Central European Cyber Security Platform 2014", *ENISA*, April 10, 2014. [Online], Available: https://www.enisa.europa.eu/news/enisa-news/central-european-cyber-security-platform-2014 [Accessed: January 22, 2019]

[8] Government of Hungary, "Government Decision No. 1139/2013 (March 21) on the National Cyber Security Strategy of Hungary", *ENISA*, March 21, 2013. [Online], Available: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/HU_NCSS.pdf [Accessed: January 22, 2019]

[9] KOVÁCS, L., *Kiberbiztonság és -stratégia*. Budapest, Hungary: Dialóg Campus Kiadó, 2018.

[10] 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], Available: http://www.visegradgroup.eu/documents/presidency-programs/slovak-v4-presidency-en [Accessed: January 23, 2019]

[11] 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], Available: http://www.visegradgroup.eu/documents/presidency-programs/sk-v4-pres-program-2014 [Accessed: January 23, 2019]

[12] Ministry of Foreign Affairs and Trade of Hungary, "Hungarian Presidency in the Visegrad Group (2013–2014)", *International Visegrad Group*, 1 July, 2013. [Online], Available: http://www.visegradgroup.eu/documents/presidency-programs/hu-v4-presidency-2013 [Accessed: January 23, 2019]

[13] Ministry of Foreign Affairs and Trade of Hungary, "Hungarian Presidency 2017/2018 of the Visegrad Group", *International Visegrad Group*, 1 July, 2017. [Online], Available:

http://www.visegradgroup.eu/documents/presidency-programs/hungarian-v4-presidency [Accessed: January 23, 2019]

[14] 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], Available: http://www.visegradgroup.eu/documents/presidency-programs/cz-v4-pres-2015-2016 [Accessed: January 23, 2019]

[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. [Online], Available: http://www.visegradgroup.eu/documents/presidency-programs/programme-of-the-polish [Accessed: January 23, 2019]

[16] 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], Available: http://www.visegradgroup.eu/documents/presidency-programs/pl-v4-pres-2016-17 [Accessed: January 23, 2019]

[17] National Cyber Security Center, Czech Republic, "Central European Cyber Security Platform 2014", *NCKB*. [Online], Available: https://www.govcert.cz/cs/informacni-servis/akce-udalosti/2140-central-european-cyber-security-platform-2014/ [Accessed: January 22, 2019]

[18] National Cyber Security Center, Czech Republic, "National Cyber Security Centre Held Exercise for CECSP Partners", *NCKB*, May 24., 2017. [Online], Available: https://www.govcert.cz/en/info/events/2532-national-cyber-security-centre-held-exercise-for-cecsp-partners/ [Accessed: January 22, 2019]

[19] National Cyber Security Center Hungary, "Megrendezésre került a Közép-európai Kiberbiztonsági Platform (CECSP) konferencia", *Nemzeti Kibervédelmi Intézet* [Online], Available: http://www.cert-hungary.hu/node/222 [Accessed: January 22, 2019]

[20] NEMETH, B., "Outside NATO and the EU – Sub-Regional Defence Co-Operation in Europe", *King's College London*, [Online], Available: https://kclpure.kcl.ac.uk/portal/files/80807208/2017_Nemeth_Bence_1212105_ethesis.pdf [Accessed: January 23, 2019]

[21] Republic of Austria, "Austrian Cyber Security Strategy", *ENISA*, March 10, 2013. [Online], Available: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/AT_NCSS.pdf [Accessed: January 22, 2019]

[22] Republic of Poland, "National Framework of Cybersecurity Policy of the Republic of Poland", *ENISA,* November 30, 2017. [Online], Available: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/govermental-program-for-protection-of-cyberspace-for-the-years-2011-2016-2013 [Accessed: January 22, 2019]

[23] Republic of Slovakia, "Cyber Security Concept of the Slovak Republic", *ENISA*, June 01, 2015. [Online], Available: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/cyber-security-concept-of-the-slovak-republic-1 [Accessed: January 22, 2019]

[24] The Czech Republic, "National Cyber Security Strategy of the Czech Republic for the Period from 2015 to 2020", *ENISA*, January 16, 2015. [Online], Available: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf [Accessed: January 22, 2019]