V4 GOES CYBER: CHALLENGES AND OPPORTUNITIES

AUTHORS:
Maroš Kirňák, Roman Šulc, Zsolt Illési, Kamil Gapiński

Visegrad Fund

SSPI Slovak Security Policy Institute

INTRODUCTION

The Visegrad Group countries (V4 – Czech Republic, Hungary, Poland, and Slovakia) are interconnected in various ways. The similar historical development and cultural similarities of the region provide a natural platform for cooperation, which carries the potential to enhance the advancement of the whole Central European region. Each country of V4 has gradually acknowledged the growing importance of cyber security issues, and the urgency to take a comprehensive approach towards addressing it, in order to protect the security of their citizens using online services while at the same time preserving the traditional values of democracy, freedom of speech, free access to information, confidentiality of information and privacy.

As a response to the emerging threats of 21th century, the European Union as well as NATO are urging their members to act responsibly and strengthen their cyber security capabilities to combat the rising number of cyber threats. As members of both organisations, the Czech Republic, Hungary, Poland and Slovakia have to adopt a complex multi-sectoral approach to cyber security, required not only to ensure an adequate level of national security, but also as a contribution to the cyber security agendas of NATO and the EU. The fact is that the Central European region remains significantly under-developed in the terms of cyber security. For several years this area did not receive the necessary political and media attention, therefore the cyber security debate is only at the beginning. Each country has different capabilities and while the Czech Republic and Poland adopted a new strategic approach and made significant progress in recent years, Hungary and Slovakia are trailing behind. The V4 countries are experiencing similar problems, which are slowing down overall progress. In many areas, these issues could be mitigated by the enhancement of mutual cooperation on a regional level. The first steps were made in 2013, when the V4 countries, together with Austria, launched the Central European Cyber Security Platform. This platform should serve as a common ground for sharing information, best practices and capacity building through joint exercises, trainings and research.

The goal of this project was to improve the coordination and efficiency of the approaches of Visegrad Group countries on matters of cyber security through research, analysis and public discussions. In cooperation with organisations from the Czech Republic - Prague Security Studies Institute, Poland - Casimir Pulaski Foundation, Hungary - Centre for Euro-Atlantic Integration and Democracy and with the support of the International Visegrad Fund, it aims to strengthen the capacity of V4 to contribute to the creation of policies on the European Union and NATO levels. During the realisation of the project, which began in January of 2016 and lasted until December of 2016, research/study trips and discussions were be held on universities in Bratislava, Budapest, Prague an d Warsaw.

The first part of the project was held in Bratislava from the 21st to 23rd of March. During this time, experts from the V4 countries met with the representatives of several institutions. These meetings also included a university lecture delivered by one of the experts at the Comenius University in Bratislava. For the second part of the project, V4 experts moved to Prague. During the three day session from the 4th to 6th of April, they met with the representatives of government as well as the private sector. They also visited the Cybergym cyber training centre. The university lecture was held at the Metropolitan University Prague. Budapest hosted the third part of the project, from the 18th to the 20th of May. The experts participating on the project met with several relevant representatives of the private and public sectors in Hungary. They also delivered a lecture and discussion with the students of Corvinus University in Budapest. On the 14th of June 2016 Warsaw hosted the fourth and last meeting of the project. Experts met with National Security Authority representatives and debated with representatives of the Ministry of Administration and Digitalization and the Casimir Pulaski Foundation.

Because all of the countries confront similar challenges, the issue division has been adopted for the purpose of this analysis. Several problems commonly found in the V4 countries will be elaborated upon, followed by our recommendations for cooperation in the field of cyber security.

DISSIMILARITIES OF THE V4 COUNTRIES

Each V4 country has a different government, different political plans and different election cycles. These governments prioritize issues differently, including that of cyber security. Each country has a different level of cybersecurity (different time of cyber initiative adoption, diverse institutional backgrounds, budget possibilities and uniquely stressed issues). Given that, V4 cooperation is complicated and at times it intensifies or is abandoned by some members, depending on the political situation.

The general stance of the Czech Republic towards security in cyberspace is driven from the inside, with the main contributing factors being the lack of major cyber incidents and the small size of the country. Despite that, the Czech Republic's approach towards cyberspace has always been very ambitious[1]. The Czech Republic was among the first European countries which have an established National Cybersecurity Strategy[2] and an updated version of the document clearly states that the Czech Republic strives to take the lead in both regional and European cyberspace contexts.

Since the parliamentary elections in Poland in October 2015, the new Polish government has been prioritizing the issues of cyber security in its political agenda. For a few months, the newly established Ministry of Digital Affairs has been conducting complex cyber security audits in terms of resources, legal and financial problems and previous actions, mostly concerning years 2007-2014. The current political agenda in Poland in terms of cyber security includes further development of the national CSIRT[3], adoption of the Act on Cyber Security until the first quarter of 2017 and speeding up adoption of relevant EU laws. It can be assumed that none of this will change, at least until the parliamentary elections in 2019. Hence, until then, Poland will remain a relatively stable partner for international cooperation.

While most of the European countries have progressed significantly in areas of security, and most of them regard this topic as one of the main security issues, in Slovakia the strategic debate concerning cyber security is only emerging. The first steps were made in 2008 with the adoption of a *National Strategy for the Information Security* , yet this included cyber security only in the broader concept of information security. Cyber related issues are not viewed as an urgent problem and were specifically addressed only in 2015 with the adoption of a new strategic approach, as a reaction to the stagnation and even worsening organisational and regulatory areas.

The Hungarian government created an cyber security framework and organisational structure to protect its cyber assets. However, due to the 2014 election and some changes in personnel, the subject was removed from the political agenda and the initial enthusiasm faded rapidly. Cyber security issues lost support and focus as new political topics–like emigration–emerged and become more important. Currently, the National Cyber Security Coordination Council, the six supporting workgroups, and the Cyber Security Forum, do not fulfil their strategic functions. Tactical organisations such as CERTS are working, but due to limited strategic support they cannot operate effectively and efficiently.

---

[1] *Tomáš Maďar: Aiming for the stars: An ambitious Czech cybersecurity approach*

[2] *National Cybersecurity Strategy Of The Czech Republic For The Period From 2015 To 2020, National Security Authority,*
source: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf, online 17.09.2016

[3] *Computer/Cyber Security Incident Response Team*

LEGISLATION

Despite the transnational nature of cyberspace and associated threats, a state only has legal authority within its own borders, what necessarily results in incoherent legislation. Despite this fact, the V4 countries are defining national cyberspace and trying to manage cyber incidents as national issues. There are different organizational structures and legal processes in place, which often makes finding solutions difficult and/or time consuming. As all the countries of V4 are members of EU, the basis of any legal framework is formed both on national and supranational levels. The European Union's approach is strongly inclined toward unifying the European cybersecurity standards, norms and procedures, which will most likely lead to mitigation of some of the incoherences between V4/European countries. Nevertheless, potential future changes will be still grounded in each nation's diverse legislation and experience.

Firstly, the Czech Republic's legal environment is constituted by the Act on Cybersecurity and its statutory instruments which were adopted in 2014. The other main source of legislation is the European Union, currently actively represented mainly by the Directive on Security of Network and Information Systems (the NIS Directive), which was adopted by the European Parliament on the 6th of July, 2016.

Under the current Polish legal framework, the key cyber security document is the "Assumptions of Cyber Security Strategy for Poland". The document has been developed by the Ministry of Digital Affairs, which is the main coordinating body for the cyber issues in the civilian area. Also, the document has to be treated as an introduction to the Act on Cyber Security, which is announced to be published in 2017. "Assumptions of Cyber Security Strategy for Poland" has the legal status of a resolution. An additional subsidiary document is the "Cyber Security Doctrine of the Republic of Poland", developed by the National Security Bureau in 2015.

Slovakia still lacks a comprehensive legislation regarding cyber security. It was the last of the mentioned countries to adopt a cyber security strategy, in 2015. *The new Cyber Security Concept of the Slovak Republic for 2015 – 2020* (further referred to here only as the "Concept")[4], alongside an action plan for the realization of the Concept were adopted as the backbone of the further development of cyber security in Slovakia. The concept modified the organisational structure and mainly initiated adoption of a new *Cyber Security Act*[5], which should fill the current legislative gap, as this area of legislation still remains significantly underdeveloped.

Hungary has a cyber security framework in place to govern cyberspace. However, this framework is not comprehensive (e.g. some important elements are not developed, such as the mandatory appointment of a cyber security officer (CIO/CSO) for each agency and annual cybersecurity audits. It also seems that Hungary is failing to fully implement its legislation (e.g. critical infrastructure is identified and assessed in a limited way and there is no critical infrastructure plan in place). Even cyberspace is incorrectly defined in the strategy as a "national cyberspace", which limits the scope of both the offensive and defensive measures and the scope of V4 cooperation.

[4] Cyber Security Concept of the Slovak Republic, National Security Bureau, source: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/cyber-security-concept-of-the-slovak-republic-1, online 9.10.2016

[5] PI/2016/58 Predbežná informácia k návrhu zákona o kybernetickej bezpečnosti, Slov-Lex, 23.06.2016, source: https://www.slov-lex.sk/legislativne-procesy/-/SK/PI/2016/58, online 9.10.2016

TECHNOLOGY

One of the very important questions is the definition of *cybersecurity/cyberdefence incident*. During our interviews, it become clear that there are no V4 or even nation-wide definitions about what constitutes cybersecurity/defence incidents. A wide range of such incidents were reported by the interviewees, while numbers of annual critical cyber incidents were between 1 - 10.000 at similar-size and type of organizations. A common threshold/template for reporting (as well as shared methodology, evaluation system and indicator sets) is also the key for successful nationwide and transnational incident handling procedures. The lack of them make it impossible to effectively and efficiently classify and manage security incidents.

In the Act on Cybersecurity, the Czech Republic defines a cybersecurity incident as an ''information security breach in information systems or security of services breach or breach or integrity of electronic communication networks resulting from cyber security event''. The definition is relatively vague and even though the associated security form used for reporting gives leeway to elaborate on the character of the incident, an adequately set general reporting threshold is crucial for the purposes of efficient data collection, analysis, adjustment of the evaluation system and effective cost and benefits analysis.

From the Polish side, it has to be noted that there is only one term introduced in the law, and that is "cyber space/domain"[6]. Definitions vary depending on the body which developed them. The significant and very confusing example refers to the term "cyber security". The "Cyberspace Protection Policy of the Republic of Poland"[7], describes "cyber security" under the term "security of the cyber domain", whereas the "Doctrine of Cyber Security of the Republic of Poland" document developed by the National Security Bureau describes it doubly as "cyber security of Republic of Poland/security of the cyber domain of Republic of Poland". Not only do each of those definitions have different names, but also some substantive differences. When it comes to the second and third definitions, it is not clear why the authors decided to include the national aspect. Knowing the specific characteristics of cyber, such a division on international and national domains appears to be risky and poorly thought out. Considering how confusing the naming might be in country's legal system, equally or even more pessimistic conclusions apply on the international level. On the other hand, it is well-known that the law is always catching up to technology and Poland is no exception. Also, part of the problem lies in the obvious limitations of languages. Putting it simply, describing the cyber phenomenon with words in any language might stand as a challenge.

In the past, Slovakia has regarded cyber security as a part or a subsystem of information security. A new approach was adopted only in the new concept, where cyber security is correctly regarded as an independent area of national security. Such adjustment of perspective also requires the formulation of clearly defined terms of cyber related issues. Absence of such a dictionary causes significant difficulties in many areas, from drafting legislation to distinguishing cyber-attacks from cyber incidents. So far, institutions work with different conceptions of cyber terms and what one institution regards as a cyber-attack another one considers to be a cyber incident, applying different incident handling procedures. Unification of the terminology is therefore necessary in order to improve intra-state as well as international cooperation.

[6] *The author of the article prefers the term "cyber domain"; therefore this particular one will be used consequently.*

[7] *strategy developed by the Ministry of Digitization and Internal Affairs, adopted by the Polish government in 2013*

The Hungarian cyber security terminology is essentially defined in the Act L of 2013 on the Electronic Information Security of Central and Local Government Agencies. However, there are some inconsistencies in the terminology, as the main focus is on the "Hungarian cyberspace" which largely limits its applicability. The act also defines the "cyber event", but organisations do not adopt and tailor this to their specific functions and operational requirements. Therefore, the number and quality of reported security incidents deviates wildly.

RESOURCES – PERSONNEL

Public agencies in the V4 countries cannot pay the same salary as market actors. Within each V4 country, there is 2–3 time salary difference between private and public IT staff. Between EU countries the salary difference is great enough to create a brain-drain and draw competent workers from V4 countries to Western Europe. V4 governments seem to neglect this, and are not attentive to it. As a result, in a long term, all V4 countries will lose their agile, well trained and skilled cybersecurity professionals, and only "secondary" staff will remain to protect the critical infrastructure.

According to the National Security Authority (NSA), which is responsible for the Czech cyberspace protection, lack of qualified personnel is one of the main resource related problems of the Czech public cybersecurity sector. The shortage[8] of cybersecurity professionals is commonly ascribed to a much smaller salary level in comparison with the private sector which can provide income several times higher. To put it in the perspective, qualified personnel at the NCSC[9] (until a special position related exam is taken) are paid about 20 000 Czech crowns, in a country where the average income nationally is 26 000 crowns per month. . Moreover, due to the legislative requirements, certain other criteria aside from one's qualification have to be met (e.g. Czech citizenship), which further limits the available pool of human resources. Security related and other demands are further reasons that potential technically skilled IT professionals from less developed countries cannot be employed to reinforce the manpower of the Czech public sector, which further widens the gulf between the state and private sectors. The knowledge gap between technical staff and decision-makers is also a problem, as well as the capability and skill differences between younger and older generations.

Poland is not struggling with a lack of qualified specialists, as a whole, but with a lack of specialists who might work under the state administration, because they too cannot offer the same salaries as the private sector. This fundamental resource issue is currently somehow being fixed, or at least being decreased in Poland. The Ministry of Digital Affairs has announced the "Golden Hundred", dedicated motivational programme for IT specialists throughout the government. According to the Ministry, one hundred specialists scattered in various departments might "have a significant impact on ensuring the required level of cyber security in the government sector (..) and have a supporting role to the non-governmental ones"[10] . Certified and experienced IT specialists will receive substantial wage benefits if they are the part of the Golden Hundred. The main goal of the Programme is to decrease the outflow of the specialists to the private sector.

[8] *Státu chybí kyberbezpečnostní odborníci a je závislý na dodavatelích, hlásí NBÚ, 28.07.2016, Lupa.Cz,*
source: http://www.lupa.cz/clanky/statu-chybi-kyberbezpecnostni-odbornici-a-je-zavisly-na-dodavatelich-hlasi-nbu, online 18.09.2016

[9] *The National Cyber Security Centre within NSA*

[10] *Ministry of Ditigal Affairs, Assumptions of Cyber Security Strategy for Poland, p. 31;*
source: https://mc.gov.pl/files/zalozenia_strategii_cyberbezpieczenstwa_v_final_z_dnia_22-02-2016.pdf

The Ministry assumes that the Programme will costs around 6 million zlotys (around 1,5 million euros)[11]. This initiative should add roughly 1200 euros to one's monthly salary. Similar anti-brain drain operations might also be taken by Ministry of National Defence. The details are yet unknown, but according to MoND representatives, special cyber security resources will be extracted from budget of the Plan of Technical Modernisation of the Polish Armed Forces in the years 2017-2022. The final sum on the cyber area might even reach 1 billion zlotys[12].

Slovakia faces many resource difficulties. Most of the government institutions are reporting a critical shortage of cyber security experts, as numbers of university graduates is insufficient to cover the current demand of the market. While this shortage is present in the private sector as well, a critical situation is highlighted in the public sector mainly due to salary differences and insufficient motivation. Demand for cyber security experts has multiplied in recent years, and private companies are offering salaries two to three times higher, compared to the public sector, while companies abroad are able to offer even higher earnings. The aforementioned gap is caused primarily by legislation which regulates salaries for the public sector. It is then not surprising that fresh graduates are less inclined to work in the public sector as it does not offer many benefits compared to the private sector. In order to attract a fresh work force, the public sector ought to offer other motivations than simply higher salaries. In the long-term perspective the situation is only expected to worsen as the share of graduates from IT sectors is insufficient and makes up only around 5% of the total number of graduates.

In Hungary there is a great shortage of IT personnel. The ICT Association of Hungary (IVSZ), which is the most important representative ICT stakeholder group covering approximately 450 top companies in the information technology, telecommunications and electronics sectors, reports 22,000 job openings currently in the ICT sector. This labor force deficiency severely affects the cyber capabilities of the country. The salary gap between the public and private sectors is more than twofold–and, especially in the ICT field, the gap is constantly increasing, mainly because of the legislative cap on salaries. Public organisations cannot catch up with private enterprises and keep losing their best personnel because of the strong competition. There is also brain drain from the more developed countries, and ICT professionals move to western Europe for higher salaries and better living conditions.

[11] *Ibidem.*

[12] *Miliard na zdolności Wojska Polskiego w cyberprzestrzeni. „Priorytet PMT";*
source: http://www.cyberdefence24.pl/444461,miliard-na-zdolnosci-wojska-polskiego-w-cyberprzestrzeni-priorytet-pmt

FRAGMENTATION OF AUTHORITIES

Cybersecurity is a fairly new field of security and its incorporation into the system of national security is slow and does not come without any complications. Dissolution of authority over this field is a troublesome matter. This unclear division often leads to confusion, ineffectiveness or even rivalry between those whose priority is to cooperate and work towards a stable and reliable level of national security.

Prior to the establishment of the NCSC, Czech cyber security was managed by the Ministry of Interior, which was in the position of the national authority for the area. This period however lasted only from March 2010 to October 2011, when NSA completely took over the agenda. The transition also applied to National CERT (CSIRT.CZ), established in December 2010, which was designated by a memorandum between its operator, CZ.NIC and the Ministry of Interior. CZ.NIC is an association of legal entities operating in the Czech Republic in the field of domain names and on the electronic communications market, which administers top-level Czech domains (.cz). CSIRT.CZ, which was originally created in 2007 as a front-runner of the Czech cyber security initiative, has been the National CERT ever since 2010. The second main body, the Czech Government CERT (GOVCERT.CZ) at the NSA, was constituted two years later. The roles of both teams in the incident handling system were specified by the Act on Cyber Security (January 2015) which designated GOVCERT.CZ as a reporting point for cyber incidents involving critical infrastructure. The rest of the entities continue to report to CSIRT.CZ as they did before. The document also formalized grounded CZ.NIC's status of a National CERT administrator on a contract basis. Aside from the Government and National CERT, Military CERT/CIRC (2007) administered by the Ministry of Defense is also present. This team is responsible for cyber defence across the Czech Armed Forces and Defense Ministry. These entities, plus about twenty other Czech private CERTs, are recognized by the international community. So far the issue of CERT proliferation, which have risen mainly in the last three years, does not seem to represent a problem, despite their relatively high number. The NCSC is currently working on the creation of new CERT/CSIRT teams both in ministries and other government offices and the industrial sphere, and support their cooperation in a private sector (mainly with critical infrastructure institutions). As a whole, the cyber security authority system in the Czech Republic[13] is rather tight and reasonably based on a long term planning, aptly chosen institutional background and the incorporation of the time-proven CSIRT.CZ entity.

[13] *National Cybersecurity Organisation: CZECH REPUBLIC, Tomáš Minárik, 2016,*
source: https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_CZE_032016.pdf, online 30.09.2016

It is quite a challenge to assess the precise cyber security competencies among the Polish government bodies. The main issue is the fact that the current strategy ("Assumptions...") has not been fully implemented yet. The Ministry of Digital Affairs proposes 3 levels of cyber coordination:

1) Strategic/policy level coordinated by the Ministry of Digital Affairs with the Ministry of Finance, Ministry of Justice and Ministry of Interior (regarding cyber crime)

2) Operational level including two contact points (both for regular and critical infrastructure operators), National Center For Cyber Security and National CERT/CSIRT alongside with sectoral CERTs/CSIRTs (energy, financial, banking, water supply, administration etc.

3) Technical Level including SOC (Security Operation Center) and end users.
Apart from what has been mentioned above , what is crucial for the system are the National Security Bureau (advising body for the president) and the Government Centre for Security. Current changes in the legal framework of cyber security lead to lower dispersion of cyber security competences. However, real changes will be feasible in the following years.

The wide fragmentation of authorities is the most visible and persistent issue of Slovakia. The field of cyber security has not found stable institutional coverage and until the creation of the Concept and Action Plan in 2015, several institutions were partially responsible for the issues of cyber security. Until then, the Ministry of Finance was the primary institution for the increase of the role of information technology in society, was also responsible for the area of cyber security.

The wide fragmentation of authorities is the most visible and persistent issue of Slovakia. The field of cyber security has not found stable institutional coverage and until the creation of the Concept and Action Plan in 2015, several institutions were partially responsible for the issues of cyber security. Until then, the Ministry of Finance was the primary institution for the increase of the role of information technology in society, was also responsible for the area of cyber security. MoF handled unclassified information and was focused on the protection of the public administration, while on the other hand classified information was under the supervision of the National Security Authority. As a primary body responsible for national security, the Ministry of Defence is responsible for the military aspects of cyber security. Critical infrastructure is under the authority of the Ministry of Interior[14]. Adoption of a new Concept made a big step in the resolution of the issue and established the National Security Authority (NSA) as a central authority for cyber security, replacing MoF. This was successfully implemented in November 2015 by an update of the Competence Act[15], which defines the organization of state service. MoF also passed on the competences regarding informatization of society, which were transferred to the newly established Office of the Vice-premier for Investments and Informatization. NSA, as a central authority, should serve as a central hub for all institutions on the matter of cyber security and is responsible for the division of tasks and responsibilities in the area at the national level, guiding MoF, MoI and other sector oriented central state authorities.

[14] National Cyber Security Organisation: Slovakia, Lea Hricikova and Kadri Kaska,
source: https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_SLOVAKIA_042015.pdf, online 9.10.2016
[15] (Act. No. 575/2001 on organization of the acting of government and organization of the central state service)

While this centralization of authority is designed to increase the efficiency and better division of resources in order to increase the level of cyber security, NSA lacks experience and it will take some time until this boost becomes noticeable. The Concept also sets up a new institution – National CERT/CSIRT. This is a new addition to already established cyber incident management and coordination structure, and is a direct subordinate of NSA. Until the adoption of the Concept, CSIRT.SK was the main response team in the civil sector, working as an independent department of Datacentrum, which was set up by MoF. CSIRT.SK directly cooperates with similar teams on the international platform (FIRST), as well as on the regional level with the teams from other V4 countries and Austria. This cooperation has proven successful and together they have launched an automatized system of threat reporting and information sharing. Suggestions for the creation of CSIRT.MIL.SK was elaborated in the Concept for Creating Capability for Monitoring, Evaluation and Measure-Taking in the Field of Information Security. This team was set up to cover the cyber needs of the military and most of its work remains classified. Unclear and fragmented division of authorities resulted intrastate rivalries. Such antagonism has led to unwilling cooperation and information sharing between national institutions. Often, international cooperation was prioritised at the expense of national cooperation. The new division of authorities might resolve the problematic fragmentation of authorities in Slovakia. While NSA does not have the capacity be the only institution responsible for cyber security, acting as a central hub for information sharing and task division to the already existing institutions might prove to be very useful.

In Hungary there are multiple organisations which handle cyber security. At the governance level there is a National Cyber Security Council, which is supported by the National Cyber Security Forum, an academic and business sector council, and some task-oriented cyber security workgroups. Besides these strategic institutes there are some sectorial Community Emergency Response Teams which are dealing with the operational responsibilities:

- the Ministry of the Interior is responsible for the central governmental incident management and established
- the National CIRT (or GovCERT);
- the Ministry of Defence is responsible for the military incident management and established the MilCERT;
- the National Directorate General for Disaster Management, Ministry of the Interior (NDGDM) is responsible for critical infrastructure incident management within its operations;
- the Hungarian Internet Service Providers (HISP) community, especially members of the Council of Hungarian Service Providers (CHIP) established a volunteer computer emergency organisation to provide services to the civil domain (HunCERT); and
- the NIIF Institute established the NIIF CSIRT workgroup to protect the Hungarian mid- and higher education and research sector.

The roles and responsibilities of these CERTs, however, are not consistently defined and there are some overlapping or neglected fields. The information sharing among these organisations is not ideal, and some of the CERTS– especially the GovCERT and the MILCERT– tend to keep secrets instead of sharing data.

CRITICAL INFRASTRUCTURE / PPP

Critical infrastructure often is owned/operated by private companies. These companies work for profit, not for the community interest. The government has the legislative power to mandate the use of cybersecurity controls. However, these measures cost money. The owners therefore argue that if the state makes something obligatory that the state must pay for it. On the one hand, private companies tend to be very flexible in adopting security measures, on the other hand their profit oriented nature sometimes compromises adoption of costly security tools and policies. Such steps are hardly tolerable from a state perspective if the lives of its citizens are at stake. As a result, there is a clash of interests between the for-profit critical infrastructure operators and the government. This is visibly present in every V4 country.

In the Czech Republic, private entities within the critical information infrastructure, particularly in the energy sector, are strongly represented. NCSC's approach toward the protection of privately owned facilities has so far been very unintrusive in respect to their owners. That agenda, however, will be likely subject to change both for the European legislations sake and the new possibilities in active defense. These will be provided by a new body which is being developed under Czech military intelligence - National Cyber Forces Centre (NCFC), which should take the reins from NCSC in most critical cases and situations (e.g. state of war). As the adopted NIS directive implies, the present-day criteria therefore establishing what is critical infrastructure will be re-evaluated in favour of a wider category approach. The Czech Republic private-public cyber environment is also characterized by a lack of cybersecurity forums which would facilitate information and experience sharing for computer security professionals from all sectors. There is the Central European Cyber Security Platform[16], which aims at the information and know-how sharing about cyber threats among its member states on a national level, but its non-public character limits information distribution. The main Czech CERT teams are also members of the FIRST (global Forum for Incident Response and Security Teams). These initiatives, however, do not include other relevant stakeholders. At least there is an information-sharing platform at the disposal of the NCSC and the critical information infrastructure/important information systems operators. Private sector entities designated as critical information infrastructure and important information systems are free to use any technology solutions as long as they are able to comply with different levels of security measures imposed upon them by the Act on cybersecurity. Standardization in incident sharing and handling is thus hard to obtain.

In Poland, from the political and strategic point of view, the Government Security Centre (Rządowe Centrum Bezpieczeństwa, RCB) conducts the policy and guidelines for the protection of critical infrastructure also regarding cyber threats. RCB is the main body when it comes to crisis management and it operates a 24/7 security monitoring centre. RCB also develops the National Infrastructure Protection Programme. RCB will serve a substantial role in the creation of network of sectoral CSIRTs (including financial, water supply and energy sector), according to the "Assumptions of Cyber Security Strategy for Poland".

[16]*Meeting of Central European Cyber Security Platform, ENISA, 10.4.2014,*
source: https://www.enisa.europa.eu/news/enisa-news/central-european-cyber-security-platform-2014, online 10.10.2016

According to the Act on the Crisis Management from 7th August 2013, selected ICT (Information and Communication Technology) systems are part of the National Critical Instructure. Operators of private and public critical infrastructure are responsible for maintaining cyber security. Moreover, if a given operator suspects the possibility of terrorist attacks (including cyber attacks) being carried out on the infrastructure it would be necessary to inform the Internal Security Agency about these circumstances to. In Poland, as in the other V4 countries, it seems impossible to maintain stable cyber security systems without the participation of the private sector. Unfortunately so far a public-private partnership model has not been effective, which is acknowledged by both sides. Sadly, even the newest strategy doesn't elaborate on the subject much. Taking the above mentioned into account, it seems fairly unlikely that such cooperation will be possible and effective within the international agenda, including between the Visegrad Group.

The troublesome division of authority regarding Slovak cyber security is also reflected in private – public partnership. In past years we have witnessed different approaches from the public sector, which left most cyber security on the shoulders of private companies. The situation concerning the protection of critical infrastructure which is vital in the protection of national security is especially crucial. But, while most of it is owned by private companies, private-public cooperation remains insufficient. Currently, incident information sharing with relevant authorities, like, for example CSIRT.SK, is not mandatory, and operates on a voluntary basis. CSIRT.SK serves to some degree as a central hub for information sharing for companies which are willing to share their information on intrusions, yet a significant amount of companies, including critical infrastructure owners, refuse to report cyber incidents. Exceptions are only Internet Service Providers, which are required to provide the incident reports to ENISA, for statistical reasons. Protection of critical infrastructure is subject to the Act No. 45/2011 on Critical Infrastructure, under the authority of Ministry of Interior, jointly with other ministries. It is the responsibility of the owner of the infrastructure to implement new protective measures and updates of the technological capabilities. Due to a lack of pressure from the public sector, the level of infrastructure protection remains inadequate as some of the owners fail to comply with current standards. Mitigation of this discord and building of a beneficial partnership requires a more proactive approach from the public sector and the building of mutual trust. This can be achieved by changing the current perception of each other as rivals, into one of partners. An initiative, drawn in Concept, to create a new public-private cooperation platform which should bring more insights from the private sector into the formulation of cyber security policies and regulations can be viewed as a positive step.

While the Act L of 2013 in Hungary requires sectoral CERTs to act cooperatively with the GovCERT, which also has the responsibility to cooperate with the private sector to promote information sharing and development of a long-term cyber security strategy, there is no dedicated public-private partnership for cyber security. There is no current political will to establish or regulate Sectoral Incident Management Centres. The ICT Association of Hungary deals with some cyber security issues, but significant companies do not play a role in the national cyber security and there is no industry-led platform to engage with such initiatives. Sometimes, mainly because of short-term financial considerations or to ease the legal requirements, the private sector is opposed to governmental cyber security initiatives.

EDUCATION AND RESEARCH

Currently the public is not aware of the real nature of, nor threats posed by, cyberspace. Poorly and inappropriately configured and managed computers, mobile phones and the Internet of Things (IoT) devices are the main attack vector and also the "ammunition" for the attackers. The situation regarding the level of cybersecurity professionals and institutions of higher education is also complicated. There are no coordinated EU, V4 or national cybersecurity related research projects in place. Current academic projects do not support security/defence hardware, software, methodology, or process development.

With the combination of the ageing Czech population and soaring dependency on rapidly evolving and all-encompassing information technologies, it is only logical that question of public awareness about threats and risks related to the use of the cyberspace and emerging phenomena such as the IoT is on the front burner. Raising the digital literacy among increasing numbers of IT users is one of the main duties of the National Cybersecurity Centre. This agenda is certainly not fully developed as new personnel responsible for the public education issue are gradually being hired. NCSC in cooperation with the Czech Police and CZ.NIC (the operator of the national CERT) operate an education and awareness raising programme which strives for the development of the information society. CZ.NIC also produces publications, educational videos, comics and other thematic materials for wider public consumption. In the long-term horizon, modernizing of the curricula for primary and secondary schools is also planned for by the Czech Republic's National Cybersecurity Strategy. The lack of cybersecurity professional education is also recognized. The Czech Republic has a shortage of undifferentiated national or sector-specific educational and professional training programs in both public and private sectors. From the NCSC perspective, attention is focused mainly on selected cybersecurity managers in a public sphere. Special courses for police experts are being prepared too. Security professionals (as well as the public) interested in self-education may also use various commercial computer security courses organized by CZ.NIC and other platforms. The lack of common computer security knowledge in professional circles is closely connected with the underdevelopment of cybersecurity in higher education. NCKS plans to monitor and promote existing academic disciplines specialised in the field of cybersecurity and help start up new ones. Basic and applied research stimulation in the Czech academic sector is also one of the continuous goals of NCSC.

It seems that in Poland both schools and academia have just started to see the need for cybersecurity education regarding both the process of shaping threat awareness and in terms of producing highly qualified IT security experts. Only a few universities in Poland offer faculty in cyber security, and only two of them (Military University of Technology and University of Warsaw) offer cryptology studies. This situation has not been changed even with the establishment of National Cryptology Centre. Unfortunately, there is not much of a policy debate regarding cyber security education. Individual higher education units in Poland may be proud of their cyber projects but it is not representative of the big picture. Regarding research, within the National Centre for Research and Development there is a special sector dedicated to cyber security innovations. Currently, two of the Centre's programmes operates in these area: "Smart Development" and "Knowledge-Education-Development". Thus, for example, the establishment of the National Cryptology Centre was possible due to the NCRD funds[17].

[17]K.Gapinski, Koordynacja potencjału ochronnego cyberprzestrzeni Polski to podstawa – pierwsza cześć relacji z debaty „Strategia Cyberbezpieczeństwa RP",
source: http://pulaski.pl/koordynacja-potencjalu-ochronnego-cyberprzestrzeni-polski-to-podstawa-pierwsza-czesc-relacji-z-debaty-strategia-cyberbezpieczenstwa-rp-2/

As much as the government is primarily involved in systematic matters of cyber security in Poland, the private and NGO sector also shares the responsibilities. Different approaches for the engagement of qualified personnel were presented by the Cyber Security Foundation In September 2015, CSF announced the creation of the "Polish Civic Cyber Defence" - using the knowledge and experience of IT security specialists from the private sector for the purposes of national cyber defence. Such volunteer initiatives have remarkable value, not just because it releases some of the financial resources, but also from the perspective of education – the "Polish Civic Cyber Defence" targets cyber amateurs as well.

Slovakia is currently implementing a project of informatization of society, with aim to maximize the usage of information and communication technologies. Usage of ICT is successfully increasing, yet it is not accompanied by the raising of public awareness and education about basic security procedures, which remains at a very low level. Several educational materials developed by the Ministry of Finance were published addressing different groups of users, yet their wider promotion through various channels (social media, newspapers etc.) was insufficient and did not reach their potential audience. More active initiatives on raising public awareness can be seen in the work of a several NGOs and online initiatives, some of them with the financial support of the European Union and Ministry of Education. Employing IT professionals, they are sharing their experiences and expertise through workshops, lectures, publishing educational material or by online consulting. The most notable are portals preventista.sk, zodpovedne.sk, and pomoc.sk. One of the contributors to the awareness rising is also CSIRT.SK, which is participating in several projects focused on awareness rising, in cooperation with CSIRTS from neighbouring countries. It also involves lectures for students in IT fields. The education of managers and decision makers in public sectors is also insufficient, as was confirmed in the Report on the Implementation of the National Strategy for Information Security 2008-2013.This is partially caused by a shortage of competent personnel who, as previously mentioned, are more attracted by private sector, as well as by the poor state of the education system. This situation was addressed in 2009 with the adoption of the *Draft of Education System in Information Security of the Slovak Republic*. This document correctly distinguishes several groups of users present in cyberspace and acknowledges different needs in terms of education. Unfortunately, this system was not fully implemented and therefore the new Concept aims to further these initiatives and improve the overall digital literacy beginning in elementary school. The situation in higher education is dissatisfying, as none of the universities offer comprehensive cyber security courses. Universities are producing insufficient numbers of graduates in the IT sector, and even fewer security experts.

In Hungary, the government cut the higher education budget in2010 and changed the operation and research model for universities. This has a serious impact on research, education and numbers of graduated students. The state reduced its contribution to research funds, leaving the EU as the main investor in the field. The research focus is mainly on physical products (e.g. hardware ready to launch on the market); fundamental research in cyber security such as algorithms, datamining etc. and applied research such as methodology or software development, are not supported.

[18] *Fundacja Bezpieczna Cyberprzestrzeń*

Secondary education discourages pupils from choosing ICT and only a small number apply to ICT related academic subjects. The university ICT student dropout rate is very high, because of the outdated university curricula and the high demand for ICT personnel (after the third or the fourth semester students can find well-paid jobs and leave). The salary gap between teachers and ICT professionals moves talented primary and secondary level teachers and academics from teaching. The salary of a freshly graduated university student can be equal to, or higher than, her lecturer, which makes it difficult to graduate the best students to masters or PhD levels, which undermines future Hungarian academic capabilities.

RECOMMENDATIONS

- **Establishment of a common approach and confidence building**

Institutions responsible for cyber security in V4 countries, despite the legal constraints, have to enhance the day-day communications as well as taking a similar approach to cyber security, regardless of the political situation. This cooperation should be established on various levels, not only currently ongoing information sharing of CERT teams. To strengthen the common approach, many confidence-building measures such as common strategies, joint exercises, collective statements, etc. are a viable option to build up stronger cyber security. A greater impulse for that will soon appear, as the European Union NIS Directive enters into force. It strongly emphasizes the common framework for critical infrastructure (essential services) protection and cross-border communication efficiency. In the efforts concerning the extension of cooperation, already existing connections and platforms would be the easiest channels to utilize, for example the extension and intensification of cooperation under the umbrella of the Central European Cyber Security Platform, or by the creation of a new V4 cyber security working group.

- **Coordinated legislation**

Although coordinated legislation would be a very welcome solution, it is unlikely that without the supranational institution or organization such political circumstances will occur. Despite this fact, the European Union and NATO could still play a productive role here. Hence, it seems possible enough to somehow coordinate some of the legislation and terminology issues, especially with respect to the NIS Directive and Enhanced Policy on Cyber Defence. The adoption of common terminology, such as that used by supranational institutions, may be a viable solution for a unified approach to cyber security. Adoption of common jargon may prove useful when applying European legislation and in international cooperation in general. As all of the V4 countries have established a cyber security strategy, the next step could be a joint V4 strategy, developed in close cooperation with the EU/NATO. The first step of such coordination could be a letter of intent that would have expressed V4 readiness for these kind of resolutions. The LoI could be initiated by the “Secure and Strong” working group experts.

- **Resources**

It is apparent that all V4 countries are experiencing a lack of cybersecurity experts in public administration, mainly due to the public salaries being lower than the private sector ones. In some cases these conditions are caused by legislation which placed various restrictions and limitations on salaries. . To attract more professionals into public service, several measures must be undertaken. Currently, demand for IT professionals from the private sector is very high and adequately rewarded. Cybersecurity, requires an even more advanced skillset. Therefore, to attract new experts governments must meet the market, in financial terms, and offer new, competitive professionals salaries. This can be done by the application of various beneficial programs, making exceptions in legislation regulating salaries in public administration or by offering other non-financial benefits such as further education, certificates, trainings, international exercises or other professional development opportunities. Applying further limitations in acquiring these positions, will prove inefficient and contrary to the intended purpose.

- **Critical infrastructure and PPP**

Considering the fact that the protection of critical infrastructure highly depends on private-public cooperation it is essential to develop a mutual trust between CI providers and state authorities. This can be executed through a more proactive approach from the public sector. It is essential that critical infrastructure provide information regarding cyber incidents, which are crucial in order to mitigate vulnerabilities and decrease the potential threat to the CI and national security. Due to the interconnection of the region, it is vital that this information should be shared within the cooperation platform of V4. One of the key elements for adequate responses on cyber incidents is to take part in regular and coordinated cybersecurity/cyberdefense practices on complex attack scenarios. These exercises should be designed with multilateral participation in mind, and private companies, academic entities and public institutions should be invited to join them as well. Practice of these scenarios provides a foundation for the development of crisis management procedures.

- **Enhancement of cybersecurity education**

The V4 should take a more proactive approach towards cybersecurity education. Current levels of cybersecurity awareness within the V4 countries is insufficient. Joint initiatives to improve this situation has the potential to gain more attention. Publication of educational materials, videos, or organisation of public events promoted through various channels to stimulate basic IT literacy may attract people of various age groups and backgrounds. As for higher education, cyber exercises with the participation of academic institutions are a very promising concept, which allows these institutions to identify trends and weaknesses and adapt their curricula accordingly. Currently existing opportunities such as students/university personnel exchange programmes could be extended to enable further development. Besides raising the of general awareness, there exists a great potential for the education of government professionals. This could be done through various exchanges of professionals to gather more expertise and experience from other countries. Various educational establishments such as CyberGym in Prague offer a comprehensive education not only for the cybersecurity teams, but also for managers and decision-makers, to connect them more with the technical side of the issue.

- **Political cooperation**

We see a space to improve the cooperation of V4 countries on several levels. The topic of cybersecurity has been absent in the meeting agendas of political elites within V4. Whether on the presidential or governmental level, high level discussion is lagging behind the current trends. Slovakia, as the President of the Council of the EU, has the unique possibility to bring this topic to the wider attention of the European Union. The same applies for the V4 platform, where the country which is currently presiding has the possibility to point the political attention to the long overlooked topic of cybersecurity. A possible improvement could be an establishment of a joint V4 working group, under the patronage of the presidents, which would serve as facilitator of the cooperation in this field.

- **Support of cybersecurity education initiatives**

Currently the general level of cybersecurity awareness is quite low and o there is a great need for providing support to already existing initiatives and enhancing the possibilities for the emergence of new ones. There is very limited number of contributors to the such awareness in the V4, which can be narrowed down to several NGOs, web portals or ad hoc lectures/events. These are supported through several funds or financed by private sponsors. There is a need to continue with this financial support for reasonable projects, in order to increase the cybersecurity awareness among the general public.

ISBN 978-80-972228-1-9
Published by Slovak Security Policy Institute, November 2016.

Partners