SAME THREAT, DIFFERENT ANSWERS? COMPARING AND ASSESSING NATIONAL CYBER DEFENCE STRATEGIES IN CENTRAL-EASTERN EUROPE

Alexander NIEDERMEIER, PhD
alexander.niedermeier@fau.de
University Erlangen-Nuremberg and Catholic University Eichstätt Ingolstadt, Germany.

Abstract

In the article, National Cyber Security Strategies (NCSS) of the Central and Eastern European states are compared and assessed. After it had become evident that a variety of crucial new threats to national security had emerged over recent years, virtually all states reacted with national strategies. These strategies are aimed at securing national cyberspace from cyber threats through legal, operational, technical and policy-related measures. They exist in addition to general national security strategies and are meant to support these. Even if most countries have National Cyber Security Strategies, the author demonstrates that these strategies show, at least in part, remarkable differences. The role national particularities play is explained, whether they are really this specific and whether they might be generalised and transferred to other national contexts and what approaches turned out best under what circumstances. Based on these results, existing strengths, weaknesses and best practices are explained to open avenues for improving existing strategies and generate a higher degree of strategy interoperability in an environment that maybe like no other requires international cooperation. It is evident that precise definitions of terms and concepts are essential. However, not all strategies provide those definitions, which might lead to misunderstandings and complicate cooperation both on domestic and international level. While some strategies offer clear cut responsibilities for the actors involved, others remain unclear. Even if laws are there to specify concrete procedures, the NCSS should not be too superficial. The NCSS itself should already make clear statements, particularly when it comes to the crucial aspect of coordinating the various cyber actors and stake holders. The author demonstrates that National Cyber Security Strategies ought

to be detailed enough to clearly determine actors and responsibilities, but open and flexible enough for adaptability to fast developments.

Key words: Cyber Security, Cyber Defense, Cyber Doctrine, Cyber Strategy, Cyber Cooperation, Central-Eastern Europe, European Union

The Universal Challenge of Cyber-Security and National Cyber Security Strategies

In mid-May 2017, the ransomware cyber-attack "WannCry" affected several hundred thousand computer systems in at least 150 states around the globe. This version of malware could infect computers without their users having to contribute actively, e.g. by clicking on a link. Europol referred to this attack as unprecedented and Arne Schönbohm, president of BSI, Germany's Federal Agency for IT-Security, spoke of "yet another wake-up call" (Fischer 2017). There is no lack of former wake-up calls and as a matter of fact, countries around the world have started to develop and refine strategies to deal with this ever-growing threat to virtually any aspect of our modern, highly-interconnected societies where practically all social activities depend on information and telecommunication technology (ICT) systems, and where with further development this dependence is most likely to increase.

Since the type of threat, which is represented by the various possible attacks in and through cyberspace, is rather new, trial and error were part of the process of developing national cyber strategies. This led to the emergence of – at least in part – quite different approaches to cyber security. First and foremost, the states' strategies focused on military aspects of cyber security. With increased knowledge and awareness of the complexity of cyber threats, the multi-dimensionality of cyber threats to today's societies had to be acknowledged. Currently, cyber security encompasses four main dimensions: cyber warfare, cyber terrorism, cyber espionage and cyber-crime. While cyber warfare and cyber terrorism primarily aim at targeting the critical infrastructure – both military and civilian – of societies in order to gain tactical or strategic advantages over the enemy and, in the case of terrorism, bring shock and awe to the population and delegitimise elected governments, cyber espionage is directed at acquiring critical information either

with respect to research and development of key civilian and military industries, or with respect to classified information of political or military importance, i.e military or state secrets. Cyber-crime may occur in various dimensions, ranging from juvenile hobby hackers to major transnational organised crime. Its main purpose is, just as any other crime, to generate monetary gain for criminals. But particularly when it comes to large-scale organised crime, the political dimension plays a crucial role, for example since the financing of terrorism can be part of cyber-crime too. On top, an increasing number of cyber-crimes may well undermine a society's effort in the realm of online banking, internet trade etc. Another form of criminal politicised cyber activity is the attempt to interfere in the interior affairs of states, particularly in the context of elections. On a larger scale, this type of activity can be seen in the context of so called information wars, which take advantage of the possibilities of cyber space for purposes of enemy propaganda.

Since all forms of illegal cyber activity have the potential to cause severe harm to the welfare and security of societies, its governments and its individuals, and to undermine civil order and delegitimise democratic political elites, national cyber security strategies (NCSS) were developed. These NCSS are aimed at securing national cyberspace from cyber threats through legal, operational, technical and policy-related measures. They exist in addition to general national security strategies (NSS; often also called White Books) as well as sometimes particular national military strategies (NMS), and are meant to support these. The existence of particular NCSS makes sense, since cyberspace, and thus cyber security, is a highly specialised realm. At the same time, it must not be regarded in isolation, since the virtual reality of cyberspace is inextricably linked with physical critical infrastructure, kinetic warfare and virtually any possible kind of socio-political and socio-economic issue.

Even if most countries dispose of NCSS, these strategies show, at least in part, remarkable differences, as comparative studies (e.g. Luiijf, Besseling and de Graaf 2013; Luiijf et al. 2013; Sabillon, Cavaller and Cano 2016) observed. This fact is interesting for two reasons: on the one hand with respect to the reasons *why* different focus points of the strategies where chosen, and on the other hand *what difference* these decisions make. In investigating these questions from a comparative perspective, one can find out what role national particularities play, whether they are really this particular or whether they might be generalised and transferred to other national contexts and, finally, what approaches turned out best under what circumstances. In other words, by comparing NCSS we can

look for existing weaknesses and best practices to open avenues for improving existing strategies and generate a higher degree of strategy interoperability in an environment that maybe like no other requires international cooperation.

As mentioned, comparative analyses of NCSS exist. They are, however, limited in two respects. First, many of these studies were already conducted some years ago (e.g. OECD 2012; Luiijf, Besseling and de Graaf 2013; Luiijf et al. 2013) and, whilst being extremely valuable at the time of their publication, they do not reflect the current state of a rapidly developing environment where most strategies have been updated or completely rewritten since. Second, in each of the existing studies we can find comparisons of strategies from various parts of the world with a strong or nearly exclusive focus on non-European states. Sabillon et al. (2016) for example compare the NCSS of Australia, Canada, the United States of America, Japan, Malaysia, South Africa and Israel while including only Norway, the Netherlands and the United Kingdom as European examples. Luiijf et al. (2013) as Sabillon et al. (2016) also analyse the strategies of Australia, Canada, the United States of America and Japan as non-European examples and the United Kingdom and the Netherlands as European examples, but add not only New Zealand but also France, Germany and the Czech Republic. In an extended study, Lujif and Besseling (2013) analyse these nations as well as India, South Africa, Uganda on the one hand, and Luxemburg, Spain, Estonia, Lithuania and Romania on the other. Shafqat and Masood (2016) offer both a comparatively current and comprehensive study analysing the NCSS of the United States of America, Canada, Australia, New Zealand, Japan, Malaysia, India, Iran, Saudi Arabia, Turkey and Israel as well as the United Kingdom, France, Germany, Spain, Austria the Czech Republic, and Estonia. All these studies generated valuable insights and offer helpful criteria for the comparative analysis of NCSS. Unfortunately, however, a region of high interest has been strongly neglected: the democracies of Central Eastern Europe. To fill this gap, the insights and framework for analysis provided by previous studies shall be used to conduct a comparative analysis of the NCSS of all Central-Eastern European states that are part of the European Union: Poland, the Czech Republic, Slovakia, Hungary, Bulgaria, Croatia, Estonia, Latvia and Lithuania[1].

1 This study comprises all NCCS of the EU member states in Central Eastern Europe except the one of Romania which was not provided in English or French language.

National Cyber Security Strategies on a Global Scale: Findings and Implications

When analysing existing strategies on a global scale, it becomes evident that most NCSS have specific aspects in common. Therefore, the aim of virtually all NCSS is to secure critical national assets and infrastructures both in the cyber and the physical realm. In general, the goal of NCSS is to protect national cyberspace against adversaries of various kinds and to enhance cyber resilience. At the same time, the aspect of respecting the fundamental rights of citizens plays an important role. In other words, the socio-political order shall not be undermined by excessive measures of cyber defence. Apart from these very general and basic notions, however, several differences between the various NCSS can be detected.

One of these aspects is a divergent understanding of central concepts such as *cyberspace* or *cyber security*. While some NCCS, as in France and the United Kingdom, operate with a wide definition of cyberspace that comprises the complete network of all virtual and physical ICT devices, others, such as in Spain, only include the internet and particular internet devices such as "classic" computers. Some NCSS even give no clear-cut definition at all. A similar picture can be found with respect to concrete cyber threats: while in Germany and France, every potential threat is part of a cyber security approach, in Finland for example, cyber security only includes the protection of digital information and critical infrastructure. As a consequence, different approaches to combatting cyber threats have arisen, which leads to difficulties when it comes to international cooperation. Even in situations when different NCSS address the same types of threats, such as cyber warfare, cyber terrorism etc., the legal assessment of cyber threats can differ quite tremendously. For example, in the NCSS of the USA, a cyber-attack is defined as an attack on digital information, ICT devices and cyber networks per se, while in Germany it refers to an attack on ICT systems that compromises the confidentiality, availability and integrity of the information systems. Varying assessments of cyber security and the cyber threat landscape make it difficult to adopt a holistic global approach. Another field of difference in definition and threat assessment is the realm of critical infrastructure. In some cases, the focus rests on critical information infrastructure alone; in most cases, however, we can find, in addition to ICT, electricity and water supply, transportation, banking and finance, national security, emergency and rescue services as well as health services

and, finally, government institutions. Sometimes, particular industrial or trade sectors as well as specific government branches are explicitly included. While the specific choice of what is classified as critical infrastructure often depends on the particularities of each state, it is clear that due to the progressing digitisation of infrastructures and the increasing sophistication of cyber-attacks, an ever-growing number of new sectors must be covered by NCSS. This again creates new challenges for finding coherent and efficient cyber security strategies. A crucial aspect in each NCSS is the matter of how to organise cyber security. In this respect, it becomes evident that there is only a little consistency as far as the departments entrusted with the task of national cyber security as responsible authority are concerned. While the United Kingdom in an exceptional way entrusted the whole cyber security of the nation to one existing body, in virtually all other cases the task of cyber security is distributed amongst multiple existing organisations working under various governmental departments. A similar pattern exists on the operational level: while nearly all countries dispose of computer emergency response teams (CERT) and information sharing and analysis centres (ISAC), there are significant variations when it comes to both missions and efficiency. The main problem in this context is the nearly ubiquitous lack of coordinating bodies that operate hand in hand with the existing institutions. When it comes to capacity building, all NCCS mention efforts to create defensive and preventive capabilities, which in practice means training measures on various levels, awareness raising in different contexts, research and development initiatives etc. In this context, most strategies focus on the development of national security-relevant products. This strictly national focus, however, again complicates international interoperability and thus cooperation. Nevertheless, cooperation is extremely crucial when it comes to cyber security. This includes both domestic cooperation between the various stakeholders that are or might get affected by cyber security issues, and cooperation on the international level, bilaterally and multilaterally, within and beyond institutional and organisational frameworks. In most NCSS, we can see provisions for close cooperation between the public and the private sector on a domestic level. In some NCSS, explicit cooperation with internet service providers is included. Unlike domestic cooperation, where often quite concrete measures can be found, international cooperation is at best mentioned as an abstract requirement, but rarely specified in the form of detailed plans or programmes. What, in comparison, do the NCSS of Central-Eastern European countries look like?

The National Cyber Security Strategies of Central Eastern European EU-Member States

Starting Points, Visions and General Aspects of the NCSS

As can be shown, comparing and assessing the NCSS of more than twenty states around the world from various regional contexts such as North America, Europe, the Middle East and Asia-Pacific delivers valuable insights into strengths and weaknesses of existing approaches and, thus, best practices and strategies for potential improvement. Taking advantage of these findings, the next step shall comprise an analysis of the NCSS of Central Eastern European (CEE) states with the aim of also detecting the best practices in the regional comparison and beyond.

When approaching the cyber security strategies of the ten CEE countries analysed, it becomes evident that all states except for Bulgaria and Hungary have distinct NCSS. While Bulgaria includes its cyber security approach in its so-called *White Paper on Defence and the Armed Forces of the Republic of Bulgaria* (Republic of Bulgaria 2010), Hungary treats cyber threats both in its general NSS (as point 31 in Part III Security Threats and Challenges for Hungary and their Management; Ministry of Foreign Affairs of Hungary 2012) and its Military Strategy (Points 33 and 33; Ministry of Defense of Hungary 2012). Based on its force structure review, Bulgaria stresses the need to revise the project for the development of a stationary communications network which is to be financed by the disbanding of garrisons and military areas. The focus is set on the integration of the stationary communications network with the networks of other ministries and agencies to create a single information network. One major goal of this endeavour is to enhance the possibilities for a wider use of commercial software products and services and the minimising of expense on software for the military. As Bulgaria, Hungary too outlines the need for a cyber security approach on the military level. At the same time, however, non-military aspects are approached. Therefore, cyber-crime or implications of disaster on cyber security are explicitly addressed as part of the national cyber security approach. In this vein, a strong focus is set on the identification and prioritisation of the various kinds of potential cyber threats

and how strengthening governmental coordination, increasing social awareness and international cooperation can contribute to tackling these threats.

The NCSS of the eight other CEE states range in length from 15 to more than 30 pages. While Estonia's current strategy (Ministry of Economic Affairs and Communication of Estonia 2014) only comprises 15 pages, it must be acknowledged that the strategy directly refers to Estonia's preceding NCSS, where a detailed programme can be found. In the current strategy, we can find a sophisticated analysis and evaluation of the previous strategy and based on this, the formulation of new goals. Since Estonia was among the first nations to develop an encompassing NCSS, the presentation of the updated measures does not require too much space. Still, it is clear that one of the main aims of Estonia's most recent NCSS is to describe methods for ensuring the uninterrupted operation and resilience of vital services, and the protection of critical information infrastructures against cyber threats. The focus is set on ensuring alternative solutions for important services and ways of managing cross-dependency between important services. The second rather short strategy paper is Lithuania's 17 page NCSS (Government of the Republic of Lithuania 2011) which significantly differs from all other NCSS. Its first five pages contain a draft of the strategy mainly in bullet-point style. The remaining 11 pages are made up of a lengthy table detailing the so-called *Assessment Criteria and their Expected Indicators* for the *Programme for the Development of Electronic Information Security (Cyber Security) for 2011-2019*. The main aspects featured in the table are 1) the objectives (e.g. to ensure the security of national information resources), 2) the respective relevant tasks to attain the objective (e.g. to improve the coordination and monitoring of electronic information security), 3) various assessment criteria (e.g. level of resources in %, the security of which is monitored by an institution designated by the law on the basic requirements related to ensuring electronic information security), 4) the indicator for the years 2011, 2015 and 2019 (e.g. 2011: 0%, 2015: 70 %, 2019: 100% in the case of the assessment criterion mentioned as example under 3), and 5) the institution responsible for implementation of the criterion (e.g. Ministry of the Interior, Ministry of National Defence, Ministry of Transport and Communications, State Data Protection Inspectorate, Communications Regulatory Authority, Police Department under the Ministry of the Interior, and Office of the Prime Minister in the case of the assessment criterion mentioned as example under 3). While Lithuania's NCSS is short, it is very dense and obviously

made primarily for administrative purposes rather than for a wider audience. At the other end of the spectrum, we find the NCSS of Slovakia and Croatia with 31 pages each. The length of Slovakia's NCSS (Slovak Republic 2015) primarily comes from the introduction where numerous definitions are provided and particularly from the long annex with further explanations and several documents including a *Framework Proposal of Tasks of the Action Plan for the Implementation* of the NCSS. Altogether, Slovakia's strategy is developed very thoroughly based on a rigorous analysis of the weaknesses of the country's up to date efforts in the field of cyber security, which – as the strategy explicitly admits – "has not been integrally and consistently regulated at a national strategic level" (Slovak Republic 2015, p. 8). The prime goal of Slovakia's NCSS, therefore, is distinguished as the creation of a system "operating conceptually, in a coordinated manner, efficiently, effectively, and on a legal basis" (ibid. 9). In this systems-approach, the notion of security awareness of all components of society and the close cooperation of the private, public and academic sectors as well as civil society and actors on the international level are particularly stressed.

The more than average length of Croatia's NCSS stems from an encompassing and very detailed analysis of cyber threats that is presented in a very logical structure where specific objectives are clearly stated. Another reason for the NCSS's length is the integration and outline of sectors such as e-government and e-finance. Croatia's overall strategic goal of ensuring quick, transparent and secure E-Government services for all citizens via cyberspace requires the establishment of a system of public registries and operating it based on clearly defined rights, obligations and responsibilities of the competent public sector bodies. The NCSS, therefore, is more than just a national security document but also the expression of a general governmental strategy of widening and deepening Croatia's socio-economic and socio-political digitalisation.

The strategic objective of Poland's NCSS appears quite modest, since it is aimed at achieving an "acceptable level of cyberspace security" (Republic of Poland 2013, p. 6, stress by author). To accomplish this objective, a legal and organisational framework and a system for effective coordination and exchange of information between the users shall be developed. The concrete measures, however, are not modest at all, reaching for an encompassing system of cyber security with a stress on organisational and structural issues. In this vein, a coherent system of cyberspace

security management for government and non-state actors as well as a sustainable system of coordination and exchange of information between the entities responsible for the security of cyberspace and the cyberspace users is about to be created. The approach is directed at building both capacity and resilience. For this purpose, the competencies of the entities responsible for the security of cyberspace are clearly defined and the awareness among the average user of the internet and respective electronic devices raised. Particularly with respect the organizational definition issue, the Polish NCSS becomes extraordinarily detailed.

The Czech Republic's strategy defines an ambitious next step moving from the building of basic capacities necessary to guarantee an elementary level of cyber security as outlined in its brief NCSS 2012-2015 towards a deeper and enhanced mode of capacity building. In this vein, the country intends to play a leading role in cyber security in Europe. For this purpose, the Czech NCSS explicitly aims at the support high technologies production, research, development, and implementation, thereby contributing to technological advancement in the Czech Republic with a view to increasing its competitiveness and creating optimal conditions for local and international investments (National Cyber Security Centre of the National Security Authority 2015, 7f.). Most outstanding with respect to a critical view as a basis for improvement is the NCSS of Slovenia. There it is acknowledged that even though there had already been several proposals concerning a systematic regulation of cyber security, no sustainable implementation had taken place (Republic of Slovenia 2016, p. 4). One of the most pressing issues to be addressed is a regulatory framework and the creation of cyber resilience. In addition, according to the NCSS, the raising of awareness of the importance of the area is required. This urgent need, however, has been met so far with a lack of political will and consensus for rapid and effective action and systemic regulation at national level (Republic of Slovenia 2016, p. 16). Nevertheless, it has become evident that Slovenia, too, is in urgent need of a NCSS. This renewed approach, which now is addressed at all stakeholders, should bring success by 2020. Aims are high: Slovenia wants to establish an effective cyber security assurance system, which will prevent and eliminate the consequences of security incidents by strengthening and systematically regulating the national cyber security assurance system, include citizens, the national economy and international partners, and address not only cyber warfare but also cybercrime and natural as well as other disasters (Republic of Slovenia 2016, p. 6).

The Understanding of Key Terms

A crucial aspect when it comes to cyber security is that all stakeholders know what they are talking about. Thus, defining key terms – at best in a congruent way for all – is of utmost importance. Of fundamental importance is the understanding of what cyber security is. Some NCSS address the term directly. The Polish NCSS defines cyber security as "a set of organisational and legal, technical, physical and educational projects aimed at ensuring the uninterrupted functioning of cyberspace" (Republic of Poland 2013, p. 5), for the Czech Republic cyber security is a process in which cyber threats in terms of cyber warfare, cybercrime, cyber terrorism and cyber espionage are identified, evaluated and resolved by enhancing the confidentiality, integrity and availability of data, information systems and other elements of information and communication infrastructure (National Cyber Security Centre of the National Security Authority 2015, p. 5). The Slovenian NCSS defines cyber security rather generally in terms of activities and measures, both technical and non-technical, that are intended to protect computers, computer networks, hard- and software and all information in this context; the NCSS explicitly includes the level of protection that is provided by these activities and measures (Republic of Slovenia 2016, p. 4). Latvia's definition of cyber security is even more general: The NCSS states that national cyber security should be viewed in the three dimensions of infrastructure, services and processes where the provision of information safety is required (Republic of Latvia 2014, p. 5). Very unlike these examples, the Slovak NCSS defines cyber security in a very detailed way as "the ability of any electronic communications network, electronic information and/or control system to resist, at a certain reliability level, random events and/or damaging activities that may negatively influence the integrity, faithfulness, confidentiality and availability of the stored, processed and/or transmitted data and/or services provided by the network or by an information or control system and thereby to disrupt and/or negatively influence the operability of, without limitation, one of the sectors of critical infrastructure and/or one of the basic security areas of operation of the state" (Slovak Republic 2015, p. 23). This definition acknowledges cyber security as a subsystem of national security that comprises not only foreign and defence policy but, at the same time, economic and social stability as well as public order and constitutionality itself (Slovak Republic 2015, p. 7). Cyber security is, therefore, regarded from a process point of view and thus understood as "a system of continuous and planned increase in political, legal,

economic, security, defence and educational awareness that includes increasing the efficiency of the adopted and applied technical and organisational measures of risk management in cyber space in order to transform it into a trustworthy environment that will provide for safe operation of social and economic processes while ensuring an acceptable level of risks in cyber space" (Slovak Republic 2015, p. 23). In a similar vein, but with a distinct focus on the individual citizen's level, the Czech NCSS states that the principal purpose of cyber security is the individuals' right to informational self-determination (National Cyber Security Centre of the National Security Authority 2015, p. 5). Estonia's NCSS also takes up this aspect when stating that "[c]yber security is guaranteed by respecting fundamental rights and freedoms as well as by protecting individual liberties, personal information, and identity" (Ministry of Economic Affairs and Communication of Estonia 2014, p. 7) and explicitly alluding to the principle of proportionality when dealing with existing and potential risks.

Just as cyber security or cyber threat, critical infrastructure (CritIs) can also be counted among those key terms that still lack a common definition and security approach. In several NCSS (such as Poland, Slovakia, Bulgaria, Lithuania, Estonia, Hungary), CritIs is not explicitly treated as major cyber threat issue. Apart from this, variations with respect to the assessment of critical infrastructure in the various Central-Eastern European NCSS also occur. While the Czech NCSS has a strong focus on industrial control systems, the Slovenian NCSS stresses the importance of the energy supply sector such as electricity producers and distributors as well as information and communication support, e.g. telecom operators and information society service providers. Other strategies, such as those of Croatia or Latvia, primarily deal with measures to address cyber threats to CritIs. Croatia's strategy is focused on increasing CritIs resilience, which means to improve mitigating the consequences of negative events such as attacks, technological accidents or natural disasters and enable fast and efficient recovery and resumption of affected systems; at the same time, however, the strategy still demands the need to determine criteria for identifying CritIs (Republic of Croatia 2015, p. 13). Latvia's NCSS, which defines CritIs as "infrastructure whose termination can substantially threaten the existence of the state" (Republic of Latvia 2014, 8f.) aims at improved communication, information and experience exchange about relevant incidents as well as distinct CritIs capacity building.

Organizational and Operational Aspects

The institutional organisation of cyber security, both on the administrative and the operational level, counts among the most important aspects of the matter, even if some NCSS do not go into great detail when it comes to organisational matters (e.g. Bulgaria, Hungary). Nevertheless, responsibility for this crucial issue often lies in many hands. While decentralisation and subsidiarity are no bad things as such, coordination is essential to guarantee efficient cyber security on all levels. As nearly anywhere else, the phenomenon of a decentralised cyber security organisation can also be found virtually everywhere in the NCSS of Central-Eastern European states. Nevertheless, we can find tremendous differences between the countries. In the case of Slovenia, for example, when the NCSS was drafted in 2016, capacities to respond to cyber threats were distributed among SI-CERT as the national response centre for network incidents, the Information Security Sector within the IT Directorate at the Ministry of Public Administration, the Ministry of Defence for defence system and protection against natural and other disasters, the Slovenian Intelligence and Security Agency in counter-intelligence activities, and the Police within its IT and Telecommunications Office and the Criminal Police Directorate, mainly in the Centre for Computer Investigations with the capacities to combat cybercrime. In this context, two problems were striking: on the one hand, apart from the Police, all institutions were lacking human, material, technical and organisational resources, on the other hand, a coordination body that would link the concerned stakeholders at the strategic level was missing (Republic of Slovenia 2016, p. 4).

This situation very much resembles the one in Lithuania where, except in the public sector, no system for the coordination of the management of electronic information security was existent when the NCSS was drafted; it must be acknowledged, however, that this had already taken place in 2011. The NCSS then names a long list of challenges: "The Ministry of the Interior has no power to exercise a proper control and coordination for ensuring the security of electronic information (cyber security), the governance and supervision structure at the level of state and public institutions is not hierarchical, the lack of cooperation among Lithuanian public and private sector entities prevents efficient planning of the development of the sphere of electronic information security (cyber security),

the existing and regularly detected vulnerabilities of information technologies, if not removed on time, give rise to the disruption of the operation of information resources as well as critical information infrastructures" (Government of the Republic of Lithuania 2011, p. 2). In reaction, a permanent collegial consultative council of electronic information security was put up, that led by the Ministry of the Interior also comprises the Ministry of National Defence, the Ministry of Transport and Communications and the State Data Protection Inspectorate.

In the Czech Republic, starting from 2011, the National Security Authority has been operating as the coordinator and national authority in the field of cyber security. In 2014 the National Cyber Security Centre was opened, which includes a fully operational CERT, the government coordination unit for rapid reaction to cyber incidents, and a national CSIRT. While Lithuania and the Czech Republic follow a strategy of relative centralisation, Croatia instead builds on the principle of subsidiarity through a systematically elaborated transfer of power to make decisions and report on cyber security issues to the appropriate authority whose powers come closest to the matter being resolved from organisation through coordination and cooperation on the technical issues (Republic of Croatia 2015: 6). Thus, the responsibility for cyber defence falls under the responsibility of the Ministry of Defence, while cyber terrorism and other cyber aspects of national security are dealt with by a small number of the competent bodies within the security and intelligence system.

In Latvia, a whole number of institutions are included in national cyber security. While the Ministry of Defence coordinates development and implementation of CIT security and protection policy through its National Cyber Security Policy Coordination Section, the National Armed Forces and the Cyber Defence Unit, the Ministry of the Interior through its Police apparatus implements the policies for combating crime, public order, security protection, and the protection of rights and legal interests of individuals. It also coordinates the settlement of crisis situations. Latvia, too, disposes of CERT, the task of which is to monitor and analyse developments in cyber space, react to incidents and coordinate their prevention, carry out research, organise educational events and training, as well as supervise the implementation of obligations specified in the Law on the Security of Information Technology. CERT also provides support for Latvian and foreign state and municipal institutions, entrepreneurs, and individuals. Both

the Ministry of Education and Science and the Ministry of Welfare pursue cyber-related tasks: While the former promotes knowledge and understanding of cyber space and its secure use, the latter implements the policy for the protection of children. Educational and awareness raising tasks are also pursued by the Safer Internet Centre of Latvia and the Latvian Internet Association. Furthermore, the Ministry of Transport organises the implementation of communication policy, while the Latvian State Radio and Television Centre, a state-owned joint stock corporation, serves as the only provider of reliable certification services, which ensures the infrastructure of electronic identity cards and electronic signatures. Further responsibilities are with the Constitution Protection Bureau that oversees critical infrastructure, the Ministry of Environmental Protection and Regional Development that organizes the governance of state ICT, and the State Regional Development Agency (SRDA) that ensures the operation and development of solutions for shared use of state ICT. With respect to the economic side of cyber security, the Financial and Capital Market Commission regulates and supervises cyber activities of members of the financial and capital market. The Bank of Latvia promotes secure and smooth operation of payment systems, while credit institutions are responsible for secure availability of electronic services in their sector. And the Ministry of Economy shall support the development of competitive cyber industries. Legal matters are with the Ministry of Justice as well as the Data State Inspectorate which develops, organises and coordinates the policy on rights in the field of personal data protection, freedom of information and supervision of electronic documents. Finally, the Ministry of Ministry of Foreign Affairs coordinates international cyber co-operation. In addition to the state actors, non-governmental organisations in the IT sector are also included in Latvia's NCSS providing support and consulting and cooperating with the Council in developing and implementing the national cyber security policy.

The Estonian NCSS-approach also works with several actors, who, however, have become more concentrated and consolidated over time. Already in 2010, the Estonian Informatics Centre was given government agency status. Renamed as the Estonian Information System Authority, it later received additional powers and resources for organising protection of the state's ICT infrastructure, and exercising supervision over the security of information systems. With respect to the protection of CritIs, the Department of Critical Information Infrastructure Protection (CIIP) was formed. Based on a CritIs mapping project, security

requirements for vital information systems necessary for the functioning of the state were developed and a CIIP commission was formed to promote public-private cooperation; for this task, it brings together cyber security and IT managers from vital services agencies to exchange operational information, identify problems and make suggestions for improving the cyber security CritIs. In 2012, the cybercrime investigation capabilities of the Police and Border Guard Board were consolidated into a single department, followed by the establishment of cybercrime and digital evidence services that were established in prefectures in 2013. The Police and Border Guard Board is also engaged in raising awareness regarding cyber threats, which, among other things, has resulted in the creation of the positions for so called web-constables the task of whom is to raise people's awareness about the security of the Internet and protect children and young people online. With respect to cyber espionage, the Estonian Internal Security Service strengthened its investigative capabilities. A strong focus was set on trans-sectoral cooperation, culminating in the creation of the Estonian Defence League's Cyber Unit. This Unit, which is made up of public, private and third sector experts, aims at improving the security of Estonian state agencies' and companies' information systems through coordinated exercises, testing of solutions, and training. It can be further engaged to support civilian institutions and protect critical infrastructure in a crisis situation.

In Poland, the entity coordinating the implementation of the Policy, on behalf of the Council of Ministers, is the minister responsible for informatisation who is to ensure coordination and consistency of actions undertaken to ensure cyber security (Republic of Poland 2013, p. 8). As operational actor, the Governmental Computer Security Incident Response Team acts as the primary CERT in the area of government administration and the civil area. Its main task is to provide and develop the capacity of organisational units of public administration of the Republic of Poland to protect against cyber threats, with emphasis on attacks targeted at CritIs. In a similar vein within the armed forces, this role is performed by the Departmental Centre for Security Management of ICT Networks and Services. In this context, it is the Prime Minister who appoints a team responsible for the preparation of recommendations concerning the implementation and coordination of any actions related to its security (Republic of Poland 2013, p. 11). In each organisational unit of government administration, as part of ensuring cyberspace security, the head of the unit should establish an information security

management system, in accordance with the applicable provisions and best practice (Republic of Poland 2013, p. 12). A remarkable institution is the Plenipotentiary for Cyberspace Security whose tasks include the implementation of the obligations arising from the provisions of legal acts relevant to ensure cyberspace security, the development and implementation of procedures for responding to computer incidents which will apply in the organisation, the identification and conducting of periodic risk analyses, the preparation of emergency plans and testing them, the development of procedures to ensure information of appropriate CERTs about the occurrence of computer incidents. Altogether, Poland's NCSS determines a three-level response system, in which the first level determines coordination, the second level incident response and the third level concrete implementation. With respect to Level 1, to ensure consistency of information security policies of organisational units, the minister responsible for informatisation in consultation with the Minister of National Defence and the Head of the Internal Security Agency prepares guidelines for information security management systems. On Level 2, the relevant actors are the Governmental Computer Security Incident Response Team and the Departmental Centre for Security Management of ICT Networks and Services, while on Level 3 it is the administrators who are responsible for the various individual ICT systems operating in cyberspace.

Slovenia's NCSS also takes a more centralist stance when it comes to the organisation of cyber security. The strategy sees the setup of central coordination of the national cyber security assurance system and provision of conditions for its stable operation. This coordination body shall coordinate the cyber security assurance capabilities at the strategic level to ensure cyber security in the country at lower levels. It represents the single point of contact for international cooperation. At the operational level of cyber security assurance, SI-CERT will operate with its capabilities at the national level, the Ministry of Defence in the field of cyber-defence, the Police in ensuring cyber security in terms of public safety and the fight against cybercrime, SOVA is responsible for cyber espionage and counter intelligence, and the emergent SIGOV-CERT for cyber security in public administration.

Another strong centralisation attempt of competencies can be observed in Slovakia, where the NCSS proposes the concentration of powers and competences of public administration bodies in the area of cyber security in the hands of

a National Security Authority. This authority shall prepare the concept of state policy in cyber security and direct its implementation in individual administration sectors, prepare drafts of generally binding regulations and methodology, and also prepare rules for accrediting incident resolution units. Furthermore, it directs the preparation of operating procedures for reactions to cyber threats at a national level, coordinates the preparation of action plans for material areas with relevant central state administration bodies, coordinates, monitors, controls and evaluates the execution of tasks in the area of cyber security at a national level, serves as the national contact point for the EU and NATO in the area of cyber security, provides and coordinates the execution of tasks implied by international cooperation, and represents the Slovak Republic internationally in the area of cyber security. In addition, the National Security Agency has the task of preparing consolidated opinions based on documents from other sectors, preparing reports on the state of cyber security in the Slovak Republic and submitting them for approval to the Cyber Security Committee of the Security Council of the Slovak Republic. In cyber crisis situations, the National Security Authority proposes and submits procedures. Finally, it continuously monitors national cyber space and analyses potential and current threats, and performs state supervision over the activities of incident resolution units (CERTS/CSIRT).

Capacity Building and Cooperation

A last important aspect with respect to cyber security is capacity building that often goes hand in hand with national and international cooperation. With respect to capacity building, NCSS again diverge sometimes significantly. While e.g. the Czech strategy remains fairly general by demanding "continuous development of cyber security expertise and of capabilities to resist the newest cyber threats" (National Cyber Security Centre of the National Security Authority 2015, p. 7) and in this vein stating that "the Czech Republic builds and continuously enhances the national expert capacities and reinforces the existing structures and cooperation procedures" (National Cyber Security Centre of the National Security Authority 2015, p. 10), other countries provide detailed approaches. Slovenia's NCSS, for example, details programmes at all levels of education ranging from pre-school awareness up to higher education, where a whole variety

of university programmes are listed that are all regarded as part of a national endeavour for cyber security. Similarly, in Poland, the research and education sectors play a crucial role in the NCSS. A particular focus is set on teachers and parents, so that from the very beginning cyber security awareness becomes part of Polish society. The Slovak NCSS admits the country's challenges in this area. It states that "[i]ncreasing awareness and education in the area of cyber and/or information security is not generally included in the educational system of the Slovak Republic (primary and secondary schools and universities) nor in the system of forming social awareness. Education is not dealt with at the level of specialised majors" (Slovak Republic 2015, p. 8). Croatia, which is confronted with a similar situation, provides a detailed action plan. Thus, the NCSS calls for the connection of all educational institutions in order to systemise programmes and curricula, increase cyber knowledge and awareness in all segments of society with campaigns including public media and by adopting cyber security as part of educational curricula for pupils, students and teachers, and encourage relevant research (Republic of Croatia 2015, p. 25). While many strategies, as shown, focus very much on education as part of awareness raising, Latvia's NCSS in addition takes a strong stance on raising professional standards and improve the labour market for cyber security experts by offering adequate university education in the field of cyber security and better working conditions for cyber experts particularly with respect to salary (Republic of Latvia 2014, 9f.). Estonia's NCSS puts the individual user in the centre of its approach, since Estonia's cyber experts are convinced that cyber security "starts with individual responsibility for safe use of ICT tools" (Ministry of Economic Affairs and Communication of Estonia 2014, p. 7). In the awareness campaigns, therefore, the focus is put on prevention. As in some other states, Estonia attempts to cover the full spectrum of education: a state-private partnership project was launched in 2013 to raise the skills and security awareness of smart device users, developers and vendors. In cooperation between Tallinn University of Technology and the University of Tartu, one of the first international Master's programmes in Cyber Security was begun, followed by a Master's programme in Digital Forensics.

When it comes to cooperation, in virtually all NCSS you can find public-private-sector cooperation as well as international cooperation. Nevertheless, differences can be observed. In Slovenia for example, cooperation of stakeholders in cyber security assurance is not formally regulated; instead, there is informal

cooperation. This includes providing information about incidents and help resolving them, the exchange of experience or the use of existing capacities. An opportunity to establish cooperation is found, however, in joint participations in the implementation of international cyber security exercises, organised by the European Network and Information Security Agency (ENISA). Such cooperation has already been established with several CritIs actors. Nevertheless, as can be taken from the NCSS, the cooperation between key stakeholders is still regarded as insufficient (Republic of Slovenia 2016, p. 16). In Poland, active cooperation with CritIs stakeholders, in particular in the fields of supply in energy, energy resources and fuel, communications, ICT networks, finances and transport, can be found. While corporations oversee their own ICT infrastructure, specific bodies are appointed for the internal exchange of information and experiences as well as the cooperation with public administration. Of particular importance in Poland's NCSS is the close cooperation with manufacturers of ICT equipment, systems, and software (Republic of Poland 2013, p. 20). While the Polish cooperative focus is set very much on the domestic level, Slovakia takes part in numerous international organisations as well as EU and NATO bodies when it comes to cyber security. Not only did the country participate in cyber trainings such as Cyber Coalition, Locked Shields or Cyber Europe, but it has established close links with the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn (NATO CCD COE), the European Network and Information Security Agency (ENISA) and the recently created European Cybercrime Centre (EC3). In the years 2013-2014, the National Security Authority fully accepted the tasks of building NATO cyber defence and information security in the Slovak Republic within the Forces Targets 2013 defence planning. With respect to domestic stakeholders, close public-private-sector cooperation including the academic realm is aimed at developing cyber-security oriented research projects. There, too, unlike Poland, Slovakia explicitly aims at joint research on a European level. Croatia, too, is developing strong links both with NATO and the EU. A major objective of Croatia is trust-building in cyber security. Therefore, the country aims at "bilateral and multilateral cooperation under existing and future agreements with international associations" (Republic of Croatia 2015, p. 23).

Latvia takes a very strong stance on international cooperation: The country takes part in international processes, including the work of NATO, EU, OSCE and UN, to promote the improvement of a secure, free and accessible cyber space.

Latvia supports the first comprehensive resolution of the United Nations Human Rights Council on human rights in the virtual space and intends to continue to participate and strengthen such initiatives as the Freedom Online Coalition, which focuses on observing human rights and basic freedoms in cyber space, especially the freedom of speech (Republic of Latvia 2014, p. 14). A very active role in shaping cyber security policy led to the establishment of the NATO Cooperative Cyber Defence Centre of Excellence in Estonia. As a matter of fact, Estonia has contributed significantly to cyber security becoming part of NATO and EU policy, having made the country something of a model. International cooperation has already reached a fairly advanced stage with successful cyber security cooperation taking place between the Nordic countries and the Baltic States, as well as with other strategic partners. Estonia is furthermore participating in additional forms of cooperation such as the Freedom Online Coalition, the United Nations Group of Governmental Experts, the OSCE informal working group on developing confidence building measures in cyberspace and many others.

Conclusion

All the states analysed have addressed the cyber security issue. Most of them have developed specific NCSS, some for the first time, some already offer an updated NCSS. In this context, the variation of the current stati between the various Central-Eastern European countries becomes evident: some stand virtually at the very beginning, still having to develop most basic structures, institutions and capacities for cyber security, others started take those steps already nearly up to a decade ago, now serving as models for the rest. In some NCSS, detailed definitions of key terms are provided. Some strategies are formulated very specifically, aimed at the relevant public administration offering highly detailed procedural steps, others are held very broadly, basically outlining an overall approach to anything concerned with cyber, including the notion of putting civic services, banking and the economy on a cyber base. Some of the latter strategies even serve as an expression of intent to develop their own industrial and service cyber industries to compete internationally on this sector. All NCSS deal with organisational and operational matters with most strategies even in very detailed ways. What becomes clear though is the very different way, cyber security is

actually organised. In some cases, we see a fairly centralised approach, other strategies go in the direction of decentralisation. A crucial aspect in all strategies in this context is the matter of coordination, both between the various institutional agencies themselves and also with respect to the cyber emergency response teams on the operational level. In all NCSS, the need for capacity building is undisputed. Most strategies put the stress on education, with most comprising the whole spectrum from young children to university level. Some strategies enlarge their approach to awareness raising to the whole population through media campaigns etc. While some strategies formulate these aims and strategies in a rather abstract way, others offer detailed procedures and show concrete developments, such as specific preventive programmes and cyber security specific Master's programmes at universities. Finally, the aspect of cooperation is dealt with in all NCSS. While in some, the need to cooperate is merely mentioned, others list several institutions and countries they intend to or are already in the process of cooperating with. While all NCSS emphasise cooperation on the domestic level between all relevant stakeholders from the public, private and academic sectors as well as CritIs, the willingness for international cooperation still differs significantly.

After comparing these strategies, it becomes evident that a precise and thorough definition of key terms and central concepts is essential. Unfortunately, not all strategies provide those definitions in an adequate way. This might lead to misunderstandings, both with respect to practical and legal issues. Therefore, it might complicate cooperation, both on the domestic and the international level, when the understanding of key aspects differs. While some strategies offer clear cut responsibilities for the actors involved, others just remain in the abstract and thus unclear. Even if laws are there to specify concrete tasks and procedures, the NCSS should not be too superficial. Particularly when it comes to the crucial aspect of coordinating the various cyber actors and stake holders, the NCSS itself should already make clear statements. The magic formula for any NCSS, therefore, seems to be what applies to any good and lasting national constitution to both determine and safeguard the values as well as the safety of society: detailed enough to clearly determine actors and responsibilities but open and flexible enough for adaptability to fast developments, in this case of the extremely fast paced cyber realm. Therefore, when updating an NCSS, looking at how the neighbouring countries have addressed issues and looking for best practices is highly recommended.

References

Fischer, B., 2017. Ein Weckruf für uns alle [14.05.2017]. http://www.faz.net/aktuell/wirtschaft/netzwirtschaft/weltweiter-cyberangriff-mit-ransomware-offenbart-weltweite-sicherheitsluecken-15013861.html.

Government of the Republic of Lithuania, 2011. Resolution No. 796 of 29 June 2011 on the Approval of the Programme for the Development of Electronic Information Security (Cyber Security) for 2011-2019, Vilnius.

Luiijf, H.A.M, Besseling, K. and de Graaf, P., 2013. Nineteen national cyber security strategies. In *International Journal for Critical Infrastructures* 9(1, 2).

Luiijf et al., 2013. Ten National Cyber Security Strategies: A Comparison. In Bologna et al. (2013) (eds): CRITIS 2011, LNCS 6983: 1-17.

Ministry of Economic Affairs and Communication of Estonia, 2014. Cyber Security Strategy 2014-2017, Talinn.

Ministry of Defense of Hungary, 2012. Hungary's Military Strategy, Budapest.

Ministry of Foreign Affairs of Hungary, 2012. Hungary's National Security Strategy, Budapest.

National Cyber Security Centre of the National Security Authority, 2015. NATIONAL CYBER SECURITY STRATEGY OF THE CZECH REPUBLIC FOR THE PERIOD FROM 2015 TO 2020, Prague.

OECD (ed.), 2012. Cybersecurity Policy Making at a Turning Point, Analysing a new generation of national cybersecurity strategies for the Internet economy.

Republic of Bulgaria, 2010. *White Paper on Defence and the Armed Forces of the Republic of Bulgaria*, Sofia.

Republic of Croatia, 2015. THE NATIONAL CYBER SECURITY STRATEGY OF THE REPUBLIC OF CROATIA, *Official Gazette* 108, Zagreb.

Republic of Latvia, 2014. Cyber Security Strategy of Latvia 2014-2018, Riga.

Republic of Poland, Ministry of Administration and Digitisation, Internal Security Agency, 2013. Cyberspace Protection Policy of the Republic of Poland, Warsaw.

Republic of Slovenia, 2016. Cyber Security Strategy, Establishing a System to Ensure a High Level of Cyber Security, Ljubljana.

Sabillon, R., Cavaller, V. and Cano, J., 2016. National Cyber Security Strategies: Global Trends in Cyberspace. In *International Journal of Computer Science and Software Engineering* 5(5), pp. 67-81.

Shafquat, Nermeen/Masood, Ashraf (2016): Comparative Analysis of Various National Cyber Security Strategies, in: International Journal of Computer Science and Information Security 15 (1): 129-136.

Slovak Republic, 2015. Cyber Security Concept of the Slovak Republic for 2015 – 2020, Bratislava.