The Czech Republic:

A Case of a Comprehensive Approach toward Cyber Space

By Lucie Kadlecová (Charles University in Prague)[1]

Daniel P. Bagge (Czech National Cyber Security Centre)

Václav Borovička (Czech National Cyber Security Centre)

Michaela Semecká (Czech National Cyber Security Centre)

[1] Work by Lucie Kadlecová was supported by the grant no. SVV–260460 / 2017.

Content

Abbreviations

CERT	Computer emergency response team
CI	Critical infrastructure
CII	Critical information infrastructure
CIRC	Computer Incident Response Team
CISA	Communication and Information Systems Agency
CSIRT	Computer security incident response team
DDoS	Distributed denial of service
DRDoS	Distributed reflection denial of service
DSP	Digital service provider
ICT	Information and communications technologies
IIS	Important information systems
ISP	Internet service provider
IN	Important network
NCSC	National Cyber Security Centre
NSA	National Security Authority
OES	Operator of Essential service

Introduction[2]

It is a generally accepted truth that cyber space is a unique socio-technical environment with a highly complex nature. Its complexity lies in the different existential levels consisting of the physical infrastructure, the code, the governing norms and principles and, of course, the layer of ideas and human creativity. All four levels combined together create cyber space, an environment toward which one has to adopt a complex approach in order to understand it. This rule applies without any exception to all interested parties, be it an individual, an international organization or a state. This report focuses on the latter while defending the need for a complex solution towards cyber space by all states with a simple goal of securing a safer cyber domain. In other words, any government and state authority aiming to build a reliable cyber security within its frontiers should adopt a comprehensive, flexible and prompt approach which would reflect the unpredictable and ever-changing character of cyber space.

A number of countries have realized the urge for this kind of solution, the Czech Republic among them. The Czech authorities made the first steps towards a safer cyber space on the national level already a couple of years ago but the real wake-up call came only in March 2013 when the Czech Republic became a target of a cyber campaign lasting several days. These cyber attacks caused a serious disruption to public life in the country that, subsequently, led to a series of complex actions by the government aiming to build cyber security which would prevent any similar cyber malicious activities in the future.

The purpose of the study in hand is, therefore, to describe the overall situation of cyber security in the country before, during and after the 2013 cyber attacks and, more importantly, to explain the processes and actions which led the transformation of the Czech Republic from a country with fairly underdeveloped cyber security to a state that has the aspirations *"to play a leading role in the cyber security field within its region and in Europe"*.[3] To do that, the study firstly summarizes the general situation of cyber security and cyber defence in the Czech Republic preceding the cyber attacks from March 2013. Secondly, it pays attention to the cyber campaign itself discussing the technical nature of the attacks, selection of targets and the immediately taken measures. Moving on, the study then focuses on the long-term development in the three crucial dimensions of cyber security and cyber defence: policy, legislation and organization. Finally, the study briefly discusses the perspectives and challenges for the future.

[2] Information in this study was checked for accuracy as of July 2017.

[3] National Security Authority, National Cyber Security Centre, *National Cyber Security Strategy of the Czech Republic for the Period from 2015 to 2020*, p. 7, available at: https://www.govcert.cz/download/gov-cert/container-nodeid-1067/ncss-15-20-150216-en.pdf.

The Czech Republic can be described as a well-connected and digitalized state with a developed dependency on the information and communications technologies (ICT). The coverage of fixed broadband in the Czech Republic reached 99 per cent of homes in 2017 and slightly exceeded the EU's average. Similarly, Czech citizens are keen Internet users as it comes to, for instance, online news (82 per cent), online banking (63 per cent) or online shopping (57 per cent). Czech businesses are not left behind. They use digital technologies to enter wider markets and keep the leading role in the highest turnover from online sales. On the other hand, the Czech Republic falls behind in certain aspects of Internet usage, such as the provision of digital public services in which it is below the European average.[4] All in all, the popularity of the Internet among Czech citizens and businesses has been constantly growing in the recent past and is currently on a good level although there is still a space for development.

The certain deficiencies in the use of Internet compared to other European countries cannot deny the level of dependency of the Czech population on Internet services which, in the past couple of years, has caused its growing vulnerability in the case of disruption. The Czech authorities have long been aware of the fact but it was not until 1 January 2015 when the comprehensive Act on Cyber Security and Change of Related Acts (Act No. 181/2014 Coll.), shaped, among others, also by the 2013 cyber attacks, took effect. Before the new Act on Cyber Security became effective, the rule of law did not specifically address the issue of cyber security in the Czech Republic. The Czech authorities had at its disposal just an inconsistent series of laws and regulations which did not cover the whole spectrum of activities in cyber space leaving dangerous blank spaces in law and policy. These legal acts covered, for example, the Act on the Protection of Personal Data (Act No. 101/2000 Coll.), the Crisis Management Act (Act No. 240/2000 Coll.), the Electronic Communications Act (Act No. 127/2005 Coll.) or the Act on Protection of Classified Information (Act No. 412/2005 Coll.). The various acts were then supplemented by constitutional law of the Czech Republic, numerous regulations and government resolutions, primary law of the EU, EU's directives and decisions and other relevant documents agreed by international community.

A similar inconsistent situation was also apparent in terms of governance. Until the establishment of the National Cyber Security Centre (NCSC), there was no institutional body which would centralize or coordinate the governance powers in cyber space. That caused a situation in which several ministries (e.g. Ministry of Interior, Ministry of Defence or Ministry of International Affairs) and government agencies exercised their powers in

[4] European Commission, *Digital Economy and Society Index 2017*, country profile: Czech Republic, available at: https://ec.europa.eu/digital-single-market/scoreboard/czech-republic.

cyber security creating overlaps and gaps. Pursuant to Government Resolution no. 781 of 19 October 2011, the Czech National Security Authority (NSA) was appointed the main authority for cyber security on the national level taking over the role of a coordinator. As part of the Cyber Security Strategy of the Czech Republic for the period of 2012 to 2015, first of its kind in the country, the NSA set two strategic and highly ambitious goals: to create the legislative framework of cyber security and to establish the NCSC. The Strategy was thus supposed to secure building of basic capacities and capabilities guaranteeing a fundamental level of national cyber security which would later serve as a basis for further development.

The NSA started fulfilling its tasks and duties immediately after the Government Computer Emergency Response Team (CERT) was established in 2012, shortly after the NSA became the national cyber security authority. The decision was taken that the NCSC would be located in Brno, Czech second largest city and the biggest tech hub in the country. The NCSC's seat was officially opened in May 2014. Together with the new Act on Cyber Security effective from January 2015, these events established an elementary level of cyber security structures in the Czech Republic, partly shaped by Czech interests in cyber space, partly by the cyber attacks targeting the Czech Republic in March 2013.

2013 Cyber Attacks

Cyber campaign in March 2013 directed mainly against Czech media, banks and mobile operators was the first and most severe campaign which the Czech Republic has faced up to now. It was also the very first test of capabilities of the newly established Government CERT and the NCSC. For the general public, it might have initially seemed that the cyber attacks were not of great importance as it meant a simple temporary denial of service; however, a lapse of time has shown that the cyber campaign would have a serious impact on future cyber security building in the country so that the government and all involved entities stand better prepared for similar or even more aggressive attacks in the future.

The whole campaign lasted for four days – from Monday, 4 March, to Thursday, 7 March – and was executed in three distinctive waves, each targeting different constituency. The first wave took place on 4 and 5 March. Czech media websites (idnes.cz, ihned.cz, Czech Television, denik.cz, živě.cz, mobilmania.cz etc.) were targeted on the first day of the campaign, while the most popular web portal and search engine in the Czech Republic, Seznam.cz, became a victim of the attacks on the following day. As a side effect of an attack against Czech Television, the website of the Regional Office of Zlín Region was down for a certain period of time during the first two days of the campaign too. The first wave of cyber attacks was characterised by SYN flood, a form of denial-of-service attack. When a user usually attempts to connect to a server, the user and server exchange a set of messages – so called "three-way handshake". First, the user sends a SYN (synchronize) message to the server requesting a connection. Second, the server replies by sending SYN-ACK message acknowledging the request. Finally, the user establishes the connection by responding ACK (acknowledgment) back. During a SYN flood type of attack, the attacker either does not send the expected ACK message back or spoofs the original IP address which sent the SYN message. That, at the end, causes that the server sends the SYN-ACK message to a spoofed IP address which is not aware of sending the original SYN message. The result is that the attacked server is flooded by messages and denies services to legitimate users.

During the second wave of the attacks on 6 March, the attackers changed their strategy. The Czech banking sector became victim of the attacks when Czech Savings Bank (Česká spořitelna) reported an incident in its network in real time followed by other banks such as Czech National Bank, ČSOB, Fio Bank and Česká pojišťovna right after the second wave of attacks was over. However, the attackers did not only change the targets of their malicious activities but also the way how the attacks were executed. The Distributed Reflection Denial of Service (DRDoS), a form of Distributed Denial of Service (DDoS), was used this time. In the DRDoS attack, the attacker sends SYN messages (request) together with a spoofed IP addresses of a victim to a large number of computers. These users reply to the request at victim's spoofed IP addresses which appears to be the source address. In the outcome, the replies are received by the targeted victim which is, subsequently, flooded by them. The DRDoS attack is, therefore, considered to be a more sophisticated type of cyber attack than the previously used SYN flood.

The third wave of the campaign came on its last day, 7 March. This time the attackers aimed their attention to mobile operators in the Czech Republic. The type of attack which they used was again the DRDoS as the previous day which made the defence against the attacks slightly more manageable. After the third wave of cyber attacks, the campaign was over and all the services and websites resume their usual business.

The Czech expert circles reacted promptly. Already during the second wave of the campaign, when it became obvious that it was not just a series of cyber attacks aiming at random targets, CESNET[5], an association of Czech universities and the Academy of Science of the Czech Republic, organized a provisional videoconference and invited all interested CERT/CSIRTs, including the Government CERT of the Czech Republic, and other expert groups. The greatest added value of such a meeting was an active participation of a senior executive from Czech Savings Bank, one of the heavily targeted banks, who shared necessary details in order to set rules on perimeter routers in real time. That helped to better regulate and, in the end, decrease the bit rate directed at servers of the Czech Savings Bank by one third. The videoconference was also used during the third wave of attacks a day later. A lesson learned was taken from the previous day when similar settings of rules on perimeter routers of affected mobile operators was adjust.

Besides the measures taken immediately during the course of cyber campaign, a series of lessons learned and potential reformative actions was identified for long-term and short-term timeframe. The long-term measures taken are discussed further in the study. The short-term lessons learned are addressed below.

One of the identified short-term actions was the articulation of nonbinding rules and guidelines for entities which might potentially become victims of future cyber attacks. The Cyber Security Council of the Czech Republic decided on one of its meetings following the 2013 cyber campaign to develop a document in this regards in cooperation with National Computer Security Incident Response Team (CSIRT). The goal of this document was to provide affected entities with recommendations on how to behave in a situation when they are under similar kind of attack and how to communicate the right information to the authorities in order to decide what the most appropriate countermeasures would be. The document was then distributed to the relevant

[5] CESNET develops and operates the Czech e-infrastructure for science, research and education which encompasses a computer network, computational grids, data storage and collaborative environment. For more details on CESNET's activities and research, visit: https://www.cesnet.cz/?lang=en.

stakeholders via the CZ.NIC and NCSC.

Another identified lesson learned, which was necessary to address in a short term, was an urgent demand for enhancement and expansion of partnership with private sector and other interested entities. This action could then be divided into two main subtasks. Firstly, there was no contact list of people responsible for IT security in big companies neither any established channels of communication for dealing with such attacks before the 2013 cyber campaign. This blank space was partially repaired when an interim contact list of responsible people in the civil service structures and in big companies was created already in the course of the cyber campaign. That immediately taken measure however could not cover the urgent long-term need for prompt cooperation with partners, preferably already during potential future attacks. The NCSC therefore set as its objective to create a contact list with names of representatives of all interested entities of civil service and critical information infrastructure who might be, in case of need, invited to convene in form of a working group, be it in person or via a videoconference, and participate on solving potential cyber crisis. This way, the NSA as a main body responsible for cyber security on the national level, would always have at its hand contact details of most of the security workplaces of government, private sector and academia and so the reaction to future cyber attacks would be more effective.

Secondly, the willingness of certain companies to share information about the attacks and their immediate coordination highlighted the fact that established trust among private sector and government authorities is the most effective tool to fight cyber attacks in real time. This trust is based on two-way cooperation. The private sector's entities should, in exchange for a reported incident, be provided with a global picture of the situation, analysis of the type of attacks and, most importantly, help to set the most appropriate countermeasures. As the 2013 cyber campaign taught us, the exchange of information, usually the most sensitive one, is very often the key to better articulate the most effective answer to a cyber attack.

To sum up, the 2013 cyber campaign against the Czech media, banks and mobile operators has been the most damaging so far although it lasted only four days and the most severe malicious action was a denial of service. No apprehensions have ever been made, neither have there been any charges. From the course of the campaign, the form of attacks used and the targeted victims, it however seems apparent that the Czech Republic served as a test bed for a campaign of potentially larger extent. Nevertheless, the 2013 cyber campaign became a wake-up call for Czech authorities that subsequently decided to take major steps in order to set or improve not only cyber crisis management but the whole spectrum of cyber security and cyber defence related measures, procedures and responsibilities.

The National Cyber Security Strategy

In the aftermath of the 2013 attacks, it was clear that cyber security in the Czech Republic had to be strengthened. A new cyber security strategy offered a perfect opportunity. The National Cyber Security Strategy for the Period from 2015 to 2020 and the associated Action Plan was adopted by the government in February 2015. The documents were formulated by the NSA, the competent authority in the field of cyber security.

The National Cyber Security Strategy in place during the attacks covered the years 2012–2015. At that time, the Czech cyber security was still in its infancy and the strategy reflected the fact. Its main focus was on building capacities necessary for ensuring a basic level of cyber security. It aimed to create a legislative framework and to establish the NCSC and Government CERT as its integral part. However, it did not go into specifics of meeting its remaining goals of protecting critical information infrastructure, strengthening security of ICT systems used in the state administration, countering cyber crime, raising awareness, or responding to cyber attacks. The strategy acknowledged importance of these but fell short of setting concrete steps and tasks for reaching the desired state.[6]

The new strategy adopted in 2015 represents an important milestone for the Czech Republic. Compared to its predecessor, it represents a qualitative shift from building elementary capabilities to ensuring the highest possible level of cyber security in the country. Besides a higher number of goals, it also sets concrete steps for reaching them. It constitutes a fundamental conceptual document, which serves as a basis for legislation, policies, guidelines and other recommendations related to cyber space protection and security.[7]

Creation of the National Cyber Security Strategy for the Period 2015–2020 was a complex process. At the time, no such comprehensive cyber strategy existed in the country and its writers had to start by looking outside the borders. Cyber security strategies of Czech Allies and countries with the same core values were a suitable starting point. By conducting a comparative analysis, the writers identified best practices and these were then modified to reflect security interests and principles as defined in the Security Strategy of the Czech Republic. A series of consultations with other stakeholders followed. Representatives of Czech ministries, intelligence agencies, military and Police,

[6] For further details, see *Strategy of the Czech Republic in the Field of Cybernetic Security for 2012–2015*, available here: https://www.govcert.cz/download/legislativa/container-nodeid-1073/20120209strategieprooblastkbnbuen.pdf.

[7] For further details, see *National Cyber Security Strategy from 2015 to 2020,* available here: https://www.govcert.cz/download/gov-cert/container-nodeid-1067/ncss-15-20-150216-en.pdf.

academia and private sector were all included in creating the Strategy and they all influenced its final form. The result is a policy document tailored to the Czech security interests.

The 2013 attacks highlighted the need to approach cyber security in a complex and systematic manner and to ensure maximum possible security in cyber space. The National Cyber Security Strategy was therefore written as a comprehensive set of measures setting down visions, principles, challenges and goals aimed at achieving the desired state.

Firstly, the Strategy puts forward a vision for the Czech Republic to become a leading nation in the field within its region and within Europe. It should be done by emphasizing continuous development of cyber expertise, by effectively securing elements of critical information infrastructure, by securing industrial control systems, or by fostering cooperation with Allies, partners and private sector.

Secondly, the Strategy stipulates the basic principles to be followed by the state in ensuring its cyber security. Since the Velvet Revolution in 1989, respect for human rights has been the cornerstone of the Czech foreign policy and the Strategy reflects the fact. It vows to protect fundamental human rights by respecting Internet's open and neutral character, to safeguard the freedom of expression, personal data protection and the privacy rights. Other principles to be followed are principles of cooperation and subsidiarity, constant cyber capability and trust building.

In addition, the Strategy lists the particular challenges and problems the country has to face. Most of them are the same challenges most of Czech Allies and partners have to counter, for example, the increasingly sophisticated malware, DDoS attacks, increase in cyber crime, shortage of cyber security experts, or Internet of Things. However, a risk the Czech Republic has to face specifically is a possibility that it will be targeted as a test bed for a major attack on its Allies or states with greater strategic importance. Such a mock-up attack could use the same techniques, tools and procedures as the real attack and therefore, the Czech Republic needs to prepare itself accordingly. After all, it cannot be ruled out that the 2013 attacks were foreplay for an attack launched in another country.

Lastly, but most importantly, the Strategy sets goals that should be reached before 2020. They were defined to reflect the visions and aspirations of the country and are divided into the following eight priority areas. Rather than to offer a complete list of specific tasks, reasoning for these priority areas is offered below.

A. Efficiency and enhancement of all relevant structures, processes, and of cooperation in ensuring cyber security

Due to the increasingly blurred lines between internal and external threats, the Czech Republic aims to coordinate all its cyber related activities so that its capabilities are used as effectively as possible, duplication is avoided and a consistent approach to cyber security issues is maintained. In this sense, the NCSC was tasked to develop a national incident handling procedure that will set a cooperation format, a communication matrix and define roles of actors involved.

B. Active international cooperation

Considering the borderless nature of the cyber space, no country can ensure its cyber security alone. The speed of developments in cyber space requires more cooperation than ever before. Therefore, the Czech Republic stands ready to actively engage in discussions in international organizations such as NATO, the EU, UN, ITU or OSCE. It is determined to deepen bilateral cooperation, including cooperation among CERT/CSIRT teams. In line with the Czech foreign policy, it also stands ready to foster an international consensus on legal norms in cyber space and on safeguarding the open nature of the Internet and fundamental human rights.

C. Protection of national critical information infrastructure (CII) and important information systems (IIS)

Critical information infrastructure and important information systems are crucial for proper functioning of a state. Recent cyber attacks in Czech neighbourhood have confirmed that elements of CII are prime targets for state and non-state actors. Therefore, protection of CII and IIS has become one of the cornerstones of the Czech cyber security. The NCSC, the main responsible body for protection of CII and IIS, is therefore tasked to continuously improve its early warning capabilities and techniques for better information sharing between the state and CII and IIS entities. It is tasked to build capacities for cyber security testing, forensic analysis, malware detection and testing, and implement a honeypot system for cyber threat detection to be developed.

D. Cooperation with private sector

The Strategy emphasizes that government powers have its limits in ensuring cyber security and that close cooperation with industry and academia is necessary. The Strategy therefore aims to create a reliable environment for information sharing, research and development and for increased trust between the government and private sector. An environment in which competitiveness of Czech companies is supported and their investments protected.

The 2013 attacks have shown that the need of close cooperation between the government and private sector is mutual. The attacks were directed against various entities. In case of such cyber campaigns, it is responsibility of the state to create a bigger picture, to put individual attacks into perspective and to adopt appropriate countermeasures preventing similar events from occurring. The more secure cyber space is, the more private entities in the country profit.

E. Research and development / Consumer trust

The Czech Republic cannot afford to be caught off guard as it was in 2013. It cannot start reacting to attacks only after they happen but needs to stay ahead of the game. Considering the constant changing nature of cyber threats, this requires continuous development of cyber capabilities and robust and resilient infrastructure. Consequently, the state shall make the research and development its national priority and shall stimulate investments in the area. It shall support the private sector and academia in their research efforts and initiate new projects.

F. Education, awareness raising and information society development

The aftermath of the attacks revealed how important it is to educate all segments of the society. Most of the countries deal with a lack of cyber security experts and the Czech Republic is no exception. As a result, emphasis has been put on creating new university programmes on cyber security. Besides the experts, the attacks have also shown the need to educate those directly affected by the events, in this case bank clients. Anyone can become a target of a hacker. By raising awareness about cyber security among all segments of the general public, from pupils at primary schools to public administration staff, potential damage of cyber campaigns can be minimized.

G. Support to the Czech Police capabilities for cyber crime investigation and prosecution

Cyber security and consumer trust will hardly be strengthened without vigorous tackling of cyber crime. Consequently, cyber crime departments of the Czech Police shall be reinforced and their equipment modernized. Also, to properly coordinate efforts in countering cyber crime, the Strategy sets goals of establishing links among the Police, intelligence agencies, NCSC and National CERT.

H. Cyber security legislation (development of legislative framework). Participation in creation and implementation of European and international regulations

To effectively ensure cyber security, the state needs to anchor it in its national legal framework. For this purpose, the Strategy aims to create comprehensive, effective and adequate cyber security legislation and to regularly assess its effectiveness. To increase cyber security of our partners, the Czech Republic is actively participating in creation and implementation of European and international norms and regulations.

Writers of the Strategy were also considering certification to be included in the document. However, after much contemplation, it has been decided that certification is to be omitted. The reasoning was that a rigid certification process could slow down development of cyber security products and services.

With the National Cyber Security Strategy is associated the Action Plan.[8] Based on the main goals of the Strategy and in coordination with all stakeholders, the Action Plan defines specific steps, deadlines, responsibilities and the supervision of their implementation. Its purpose is simple - not to let the strategy become a document of empty words. The aforementioned tasks were formulated in such a way that all would be feasible and that it would be possible to assess whether they were met or not. To that end, the NSA conducts an annual assessment of the tasks. The output is a report informing the government and general public on effectiveness of measures adopted and on progress in fulfilling the tasks defined by the Strategy. The report is annexed to an annual Report on the State of Cyber Security in the Czech Republic. According to the last assessment from the year 2016, stakeholders are continuously fulfilling the goals imposed on them by the Strategy.[9]

[8] Document *Action Plan for the National Cyber Security Strategy of the Czech Republic for the Period from 2015 to 2020* is available at: https://www.govcert.cz/download/gov-cert/container-nodeid-578/ap-cs-2015-2020-en.pdf.

[9] The Report on the State of Cyber Security in the Czech Republic in 2016 is accessible at: https://www.govcert.cz/en/info/publications/2534-report-on-the-state-of-cyber-security-of-the-czech-republic-2016/.

Legislation

In 2011, it became clear that government's cyber security policy is not fully functional. The government's approach to cyber security was scattered as the issue was dealt with only marginally and not within necessary complexity. On 19 October 2011, the government issued a regulation which reacted to that situation. First of all, the NSA was appointed as a national authority for cyber security and was given initial competences in this field. It was also decided to create the NCSC and the new legislation in this area.

The first outline of the new law was introduced in June 2012. The main task was to:

(i) create a system of entities upon which the cyber security of the state is the most dependent and give them specific obligations in this area;

(ii) set legal competences of NSA in cyber security field;

(iii) create legal prerequisites for operating of Government CERT (GovCERT.CZ) and National CERT; and

(iv) create a system of information sharing between all relevant subjects.

Creation of the Act on Cyber Security

The concept of the Act on Cyber Security was approved by the government and first proposal was sent to the Parliament in January 2014.[10] The legislative process was rather smooth, as both ruling and opposition parties agreed on the need to adopt such legislation, realizing the necessity to create a comprehensive state policy in this area. In July 2014, the Act No. 181/2014 Coll., on Cyber Security (the Act), has been adopted by the Parliament and entered into force on 1 January 2015.

One of the crucial elements during the preparation of the Act was the intensive cooperation between public and private sector and academia. The academia brought the proper legal theoretical background and ideas on conceptual issues. The private sector, on the other hand, had a lot of opportunities to comment the text of the Act from the practical perspective and propose their own ideas on how the cyber legislation should be built. All this had several very positive outcomes.

First, the proposal was scrutinized by IT companies, experts and practitioners themselves. The experience and from-the-bottom perspective brought the law closer to praxis and

[10] The time gap between submitting the outline to the government and submitting the proposal to Parliament was caused by political crisis which led to government's resignation followed by early elections to Chamber of Deputies of the Parliament of the Czech Republic.

removed several misunderstandings caused by a different language and perspective of legislators and IT experts.

Second, the law was prepared in the time of several foreign state-surveillance scandals. These also had negative impact on the perception of the state activities in cyber space by general Czech public. It was therefore very important to be open about the law and its impacts. By giving the public wider possibilities to talk into to the final form of the law, the Act was not being seen purely as an authoritative piece by the NSA, but rather a cooperative outcome of a number of subjects involved both in private and public Czech cyber security domain. The fear from surveillance intentions or intentions to somehow restrict the freedom in cyber space has been reduced.

Third, the cooperation itself provided effective spread of information about the Act among the broader population and, importantly, gave a very solid basis for further development of good relations between public and private sphere during the implementation of the Act. On a number of occasions, such approach has been publicly highlighted by several institutions as a good example of a proper communication, contributing to building trust between the NSA as a cyber security authority and public institutions and private companies as regulated entities.[11] The NSA still profits from this approach during the ongoing implementation period; it is possible to observe that institutions and companies are more open to cooperation.

Another worth-mentioning thing about the creation of the cyber legislation was the change in the perception of some private companies caused by relatively wide cyber attacks from March 2013. During these attacks, there was no proper information sharing about cyber security incidents between relevant subjects. Especially private companies experienced the need for complex and relevant information about the scope and intensity of attacks. This also helped to shift the rather sceptic professional public attitude towards cooperation on building a proper cyber security system.[12]

[11] Trust between all subjects important for the cyber security of the state is also projected into the Act, see below.

[12] Martin Nováček, „Právo o páté: Radim Polčák - koordinace obrany před kybernetickými útoky je potřeba," *Pravniprostor.cz*, 2014, available at: http://www.pravniprostor.cz/clanky/ostatni-pravo/pravo-o-pate-radim-polcak.

The Principles

The Act itself is built on several principles which are reflected throughout the Act as well as considered to be special guiding parameters for the activities of the NSA in the cyber security field. The explanatory report to the Act mentions the following principles:

Technological neutrality

The principle of technological neutrality can be divided into two sub-principles.

First, the Act (and the activities of the NSA) aims strictly on the technology and is not concerned with the content of the information which are processed or transmitted through cyber space. The main objective is the infrastructure and its proper functioning. Beside the fact that this helps the NSA to be more focused on specific problems associated with the functioning of cyber space and its important networks and systems, it significantly contributes to increasing the trust of obligated persons and institutions in the NSA and its activities. Being aware that the NSA does not address the content of the information of the obligated persons and institutions, but merely the security measures and cyber security incidents and threats, they are more willing to share the information about incidents and ways to stop them and prevent them. The confidentiality of their information is much more assured.

Second, the Act does not prefer one specific piece of technology or technological process over the other. It merely says what measures need to be taken to protect networks and systems, but does not say how they should be taken and what technologies exactly should be implemented. The reasons are both security and economical. By stating only the result of each security measure, companies and institutions are encouraged to find their own security solutions which fit specifically for their system. Due to this principle, the subjects are not forced to stick with only few technological options, on the contrary, it particularly promotes new and innovative solutions how to protect important systems and networks. Technological neutrality also ensures that the internal market and necessary competition is not distorted by preferring one solution over the other. Last but not least, this approach is politically neutral which also did not cause disputes over the law in this respect.

Protection of informational self-determination

Information self-determination is considered to be key element which is protected by the whole cyber security legislation and by activities of the state in this field. Originally, right of information self-determination has been seen merely from the passive perspective, i.e. that state should ensure protection of human's privacy and his personal data. Nowadays, active element of this right is promoted as well – humans have right to actively create, send, receive and process the information. The possibility to communicate with others and share information is important part in human's life and state should therefore protect it.[13]

Protection of non-distributive rights

This principle is partially connected with the previous one. State has a right to protect its own security and has to be capable of creating and sustaining safe living conditions for its people. The Act pursues this idea by creating a system which contributes to cyber security and therefore to security of the state itself.

Minimization of state's coercion

The scope of the Act does not comprise all networks and systems under the Czech jurisdiction, it rather determines only those systems and networks which are highly important to fulfil above mentioned principles. The set of obligations is also different for different types of regulated entities, according to their importance.[14]

Moreover, the objective of the Act is not the state's repression. Generally, the repressive approach towards cyber security in the sense of the Act would be very ineffective. Without a trust and cooperation, the system would not work properly since it would be extremely difficult to share information about cyber security threats and incidents. The Act follows the opposite direction as it embeds the principle of minimization of state's coercion into one of the main pillars of the Act; cooperative approach better enables to create trust between the state and private sector.[15]

Autonomous will of the regulated entities

Principle of autonomous will of regulated subjects is closely connected with the technological neutrality principle as it gives subjects a free choice on how to fulfil the security measures stated by the Act.

Due diligence towards other states and international society

[13] At the time of writing, an English version of the Explanatory Report was not available. The Czech version was used for reference instead. Explanatory Report of the Act on Cyber Security and Change of Related Acts, pp. 48–49, available at: https://www.govcert.cz/download/aktuality/container-nodeid-571/nbu-zkb-navrh-140102-vlada.pdf.

[14] Ibid, p. 50.

[15] Within the forthcoming amendment of the Act, it is proposed to increase the sanctions, since current fine is rather low which is misused by a small number of regulated companies. Despite this fact, the principle of minimization of state's coercion is still valid as the discretion authority over the amount of the fine NSA is still affected by this principle.

Adoption of the Act on cyber security have not had only domestic purpose but also international one as it expresses the commitment of the Czech Republic to observe the norms of international public law, specifically the due diligence principle. The state is obliged to actively prevent internationally wrongful activities emanating from its territory. The creation of a minimal cyber security system with generally set standards represents an active approach of the Czech Republic to prevent cyber attacks on other states originating from the Czech territory. Consequently, it could help protect the state by minimizing the state's responsibility for breach of the due diligence principle.

There are also some principles which are not directly mentioned in the explanatory report, however, their importance is implicitly accepted. Those principles are:

Principle of individual responsibility of the owner for the security of its own system and network

Since the Act builds upon trust, cooperation and free will of regulated subjects and minimization of state's coercion, naturally, one other principle is implicitly included in the Act. That is that the main responsibility for the security of systems or networks still lies upon the owners themselves and they should actively do so. So even though the Act creates the conditions for functioning of governmental and national CERT, they should not replace the activities of system and network owners. The Act does not take away the natural duty of regulated subject to protect their services.

Principle of cooperation and trust

The last but very important principle is the principle of cooperation and trust. As was mentioned above, the trust between the NSA and regulated subjects and between all subjects, which could share information about incidents and know-how to protect from them, is essential. The subjects themselves need to understand (as they do) that sharing information and cooperating with others is for their own benefit. On the other hand, from the position of the state, to control fulfilling of all security measures set by law would be extremely difficult without necessary cooperation; without necessary trust the system would not work properly.

The principle is expressed in many activities of the NSA. For example, security audits carried out by the NSA according to the Act are rather helpful as their primary aim is to help subjects to better secure their systems and networks, not repressive ones attempting to look merely for errors and faults to impose penalties. During the security audit, the NSA not only evaluates faults in security, but also highlights great solutions and impressive efforts in securing systems and networks. Such "auditing to improve" approach is not very common in other parts of the Czech state's administration.

Regulated Entities

Entities, which are regulated by the Act, are (a) Electronic communication service provider and entity operating electronic communication network, (b) Operator of important network, (c) Operator of critical information infrastructure information system, (d) Operator of critical information infrastructure communication system and (e) Operator of important information system.

From the beginning, the main purpose of the Act was to protect the vital systems first, therefore the core regulated entities are operators of critical information infrastructure (CII). These are defined by Government Decision no. 432/2010 Coll., on the Criteria for the Determination of the Elements of the Critical Infrastructure (CI Decision) which relates to general crisis management legislation. Generally, the CII are those systems which are essential for operating Critical Infrastructure (CI). For instance, if a nuclear power plant is identified as CI,[16] then those systems and networks which are essential for operating the plant are determined as CII. CI Regulation also gives some other criteria for CII that go beyond CI, therefore a vital system could also be present outside the current CI system. If a system fulfils the criteria, a special decision is issued and operators of CII have to comply with the Act and implement a full scope of security measures given by Regulation No. 316/2014 Coll. on Security Measures, Cyber Security Incidents and Reactive Measures (Cyber Security Regulation).

In order of importance, the other type of regulated entity is an operator of important information system (IIS). IIS overcomes the gap between the importance of CII and other types of systems. The determination criteria for IIS are present in regulation No. 317/2014 Coll. on the Determination of Important Information Systems and Their Determination Criteria (IIS Regulation).[17] Also, the operator of such a system needs to be an entity of public authority. The reason behind this solution is that it is mostly public entities which very often do not have sufficient capacities and funds to properly secure their systems. By including them in the Act as regulated entities, they are obliged to implement security measures as stated in Cyber Security Regulation and therefore are entitled to obtain money from public budget for such activities. Private subjects, on the other hand, are not included due to the minimization of state's coercion principle. State wants to interfere

[16] Determination criteria for CI are also included in CI Decision. Beside special sectoral criteria, all CI (and CII) has to fulfil at least one of the following cross-cutting criteria: The disruption of the element/service can cause: (i) more than 250 casualties or more than 2 500 persons with subsequent hospitalization for more than 24 hours; (ii) economic loss higher than 0,5 per cent GDP; (iii) restrictions on the provision of essential/vital services or other serious impact into everyday life, affecting more than 125 000 persons.

[17] IIS has a different determination process than CI; therefore, the criteria are set by a different implementing regulation.

with rights of private subjects as little as possible, therefore unless a private subject operates CII, the Act does not include it among IIS, which consequently means that the state does not impose the obligations to implement security measures according to Cyber Security Regulation.

Next type of regulated entity is an operator of important network (IN). In short, INs are those networks providing direct international interconnection to public communication networks or providing direct connection to critical information infrastructure. In other words, operators of INs are more important internet service providers (ISPs). At the same time, their obligations according to the Act are a bit higher than obligations of ordinary ISPs.

The last and probably the most common type of entities regulated by the Act are electronic communication service providers and entities operating electronic communication network, i.e. ISPs. The number of registered ISPs in the Czech Republic is high and, in vast majority, they are in private hands. Following all principles and necessity and effectiveness of regulation, ISPs have the least number of obligations according to the Act. A mere report of contact information to National CERT is actually the only obligation they have. The idea behind this approach is that, on one hand, ISPs constitute basic elements of the "Czech Internet" and it is necessary to be able to get in touch and effectively communicate with ISPs when dealing with cyber security incidents. On the other hand, as individual ISPs are usually not vital elements[18] of Czech cyber space, it is not necessary to impose more obligations upon them. At the same time, the security of their systems is essential for their business and therefore their intensified strive for security is presumed. This "light touch" approach, however, applies only during normal operations; if a cyber crisis comes and the state of cyber emergency is declared, ISPs might be subject of further obligations.

Obligations

The Act gives four basic types of obligations: (i) to report the contact information to competent CERT, (ii) to detect and report cyber security incidents to competent CERT, (iii) to implement security measures, and (iv) to implement reactive and protective decisions of the NSA. First, reporting of contact information is a basic obligation given to every regulated subject, since only proper communication with right contacts can be effective when dealing with cyber security incidents or during crisis. Second, the

[18] If an ISP should be a vital element, it will fulfil the criteria for IN or CII and will follow the respective rules.

obligation to detect and report cyber security incidents is given only to operators of IN, IIS and CII (but in fact, most of the common ISPs detect incidents as well).

Third, security measures according to Cyber Security Regulation are seen as a basic element of protection of IIS and CII and therefore must be implemented by these two types of regulated entities. CII has to observe full scope of Cyber Security Regulation, while IIS have set a lesser level of implementation. The measures were laid down while realizing the principles upon which the Act is built. It was no purpose of the Act to give obligations to implement new or special and infrequent measures. On the contrary, the security measures follow the line of best practices of information security management and officially admit the inspiration in ISO 27001 standards. By this approach, the regulated entities do not face anything new as many of them already owns the ISO 27001 certificate or act according to best practices included in these norms. At the same time, these security measures are scrutinized by expert public and are considered as basic stones of information security management system.

Finally, reactive and protective decisions are the last category of obligations for regulated entities. Reactive decision is a decision issued by the NSA to one or more regulated entities to "*solve cyber security incident or to secure information systems or networks and electronic communication services from cyber security incident*".[19] In other words, if there is a threat of a cyber security incident or an ongoing incident, the NSA can issue a decision in which it orders a regulated entity to make a certain action to stop or prevent such incident. Since such authority is rather considerable, the NSA is still limited by the above-mentioned principles. Therefore, the NSA would issue it only in situations where it is necessary and where a cooperation approach is not effective to deal with the incident. Protective measure, on the other hand, is issued on the basis of an analysis of an already solved cyber security incident. It contains an obligation to an action which increases the security of the system.

Government and National CERT

As it has been mentioned before, the Act creates legal prerequisites for operating of Government CERT and National CERT. Both of these are cyber security teams presumed by the law, with different scope of activities and competences. Government CERT is a security team run by the NSA, i.e. it is a public authority body. The main constituency for

[19] Act No. 181/2014 Coll., on Cyber Security and Change of Related Acts, § 13 paragraph 1, available at: https://www.govcert.cz/download/legislation/container-nodeid-1122/actoncybersecuritypopsp.pdf.

Government CERT is CII, IIS and the rest of public administration. National CERT is a security team run by a legal person, not a state. The legal person is selected during a special kind of procurement. Its main focus is on ISPs, INs and other private sector subjects. In general, with few exceptions, it can be said that Government CERT aims on the public-sector institutions and CII, whereas National CERT is primarily designed as a contact point for ISPs and private sector. The competences are similar – they are obliged to receive reports about cyber security incidents, evaluate them and provide methodical support, help and cooperate with other subjects.

The reason for such a division is fourfold; first, the trust of the public in the state was not very high in the beginning. The creators of the law were worried that mainly private subjects will not report the incidents to a state body due to the lack of trust that the sensitive information would not be leaked. National CERT, as a proven and trusted private entity, would be credible for other private entities. At the same time, it would be possible to ensure the protection of information by a separate non-disclosure agreement; the Act does not forbid such additional agreements in this area.

Second, the private sector has had some expert capacities in cyber security which is very difficult for the state to obtain. By creating National CERT, it allowed to include a private institution with a strong expertise into the Czech cyber security system and hereby use the expertise for public benefit. Even now, when initial expertise is created in Government CERT, the close cooperation with National CERT allows to share know-how and creates synergy when dealing with today's cyber threats.

Third, National CERT could serve as an established and skilled backup in situations when Government CERT would not be able to act. Since Government CERT is a public authority body, it can carry out only those activities which the Act prescripts. National CERT, on the other hand, as an institution of private law, can do everything unless the law says otherwise. Cyber space is rather dynamic area whereas legislation is very slow and usually is not able to react quickly enough to deal with new threats. Even though the Act is written in simple manner to embrace as many situations as possible, it cannot presume all eventualities; therefore, the division serves also as a safeguard for unforeseeable situations when Government CERT (as a last resort capacity) would not be able to act due to the lack of legal competences and National CERT would be able to compensate that insufficiency.

Fourth, National CERT as an entity of private law and Government CERT as a public authority body are presumed to cooperate partially with a different set of partners. For example, it is easier (and more natural) that cooperation with Allies within NATO should be responsibility of a state body, i.e. Government CERT, not a private entity. The same applies to the cooperation with intelligence services. On the other hand, a number of formal and informal collaboration within a cyber security community is carried out only between private entities. Some communities of experts do not trust the states and their institutions. In some cases, therefore, having a private entity included in the pillars of Czech cyber security system can enable larger reach into the different parts of cyber security community and could bring more solutions and information on how to protect the state's systems and networks.

State of Cyber Emergency

The presence of cyber threats grows and the incidents tend to be more and more severe. When a state faces an extensive DDoS attack aiming on various systems of different sectors, usually one of the effective way to thwart those attacks is through coordination with ISPs which provide connection of systems to the global Internet. The Act, however, in normal situations does not address any special obligations to ISPs, nor gives competences to the NSA to issue any kind of order towards them. Therefore, a state of cyber emergency had been presented in the first official draft of the Act.

State of cyber emergency is defined as "*a state, during which information security in information systems or security and integrity of services or electronic communication networks is seriously endangered and the interests of the Czech Republic may thus be violated or endangered* [...]".[20] It can be declared by the Director of the NSA for up to 7 days, with possibility of further prolongation up to 30 days. If a state of cyber emergency is declared, such information has to be published in communication mass media; television and radio broadcasters are obliged to publish such information without delay and with no content and meaning adjustment. By this measure, it shall be ensured that the information gets broad public attention. Public awareness about on-going cyber crisis could consequently help carry out some necessary actions of affected subjects (i.e. implementing some special security measures) and adjust people's behaviour on the Internet.

Besides the "awareness function", declaration of the state of cyber emergency gives the NSA competence to issue a reactive order towards ISPs to make them do a certain action with the aim to handle the cyberattack. Hereby, the NSA has an authority to intervene into ISP's operations and impose specific measures which ISP must take. In practice, this measure will be used exceptionally; generally, the cooperation between main ISPs and CERTs works well and the measures could be usually taken on a recommendation basis. At the same time, it is very delicate to impose specific actions and interfere with foreign system.

[20] Act No. 181/2014 Coll., on Cyber Security and Change of Related Acts, § 21 paragraph 1, available at: https://www.govcert.cz/download/legislation/container-nodeid-1122/actoncybersecuritypopsp.pdf.

In March 2013, when rather large DDoS attacks were carried out against various systems located in the Czech Republic, the Act was being in the legislation process and there was no legal mechanism for cooperation between ISPs and, at that time newly created, National and Government CERT. The proposed provisions of the Act showed therefore their purpose. In a way, it can be said that 2013 attacks showed that the Czech Republic took the right way creating the cyber security legislation.

NIS Directive and Further Development

On 6 July 2016, the European Parliament adopted the Directive on Security of Network and Information Systems (the NIS Directive). The effort of the EU to create and implement NIS Directive had been publicly known during the creation of the Act. Its main concept, therefore, attempted to correlate with the purpose of the NIS Directive. Some provisions have been, however, not included in the Act since the NIS Directive further evolved in the time between the adoption of the Act and adoption of the NIS Directive.

Due to this situation, the Act went through an amendment process as some of the NIS Directive provisions needed to be included into national legislation. The main change can be found in the area of regulated entities. The Act newly presents Operator of Essential Service (OES) and Digital Service Provider (DSP). OES is, by definition, very close to CI; the OES systems have similar set of obligations as CII. At the same time, OESs are not connected to Czech crisis legislation and are treated merely from cyber perspective. DSPs and their obligations are regulated according to the NIS Directive.

Besides the implementation of the NIS Directive, the opportunity has also been taken to fix some technical problems of the Act and solve some of blind spots in ensuring cyber security of the state.

At the same time, another amendment process of the Act has taken place. The main purpose of this amendment has been to set the legal obligations for suppliers of CII, IIS and newly defined OES to secure their systems used for the supply the similar way as is the obligation for the owners of the CII, IIS or OES systems.

The amendments came into force in the third quarter of 2017 with related regulations being currently in the legislation process.

To conclude, it is important to note that the Act is not the only part of the law which deals with cyber issues. Many other acts set standards of behaviour of people, legal entities and public authority entities in cyber space indirectly. For example, according to penal code, it is forbidden to do certain activities like "unauthorised access to computer systems and information media" or "theft". On the other hand, we can also find a crime of "damage and compromise of operation of publicly beneficial facility", which could apply for successful attacks on CII. By putting these offences into the Criminal Code, state expresses the limits of peoples' behaviour and hereby sets state's policy in this area. Similar offences can be found even in Civil or Administrative laws.

To sum it up, the main Czech cyber security legislation is built upon the Act No. 181/2014, on Cyber Security and supported by individual cyber-related provisions in other parts of Czech legislation. In recent months, the Act proved itself as well created and functional as the principles, regulated entities and their obligations have been duly set. Further development will be influenced by the practical results coming from current amendments of the Act.

National Organization of Cyber Activities

As all states, the Czech Republic faces cyber attacks of various kinds and to face them effectively, it must clearly define and determine its cyber organizational structure. This chapter aims to present a comprehensive picture of state's cyber activities. It outlines a distribution of responsibilities for cyber related tasks and rationale behind the distribution, describes tasks and competencies of individual cyber institutions and areas of cooperation among them.

The key to the organizational structure of cyber activities in the Czech Republic is a clear distinction between cyber security, cyber defence and cyber crime, and this chapter is divided accordingly. It starts with the Czech understanding of cyber security and description of competencies of the national authority in this field. The same is subsequently done with cyber defence and cyber crime. To complete the picture and conclude the chapter, the last section deals with interagency cooperation as the ability to cooperate and fill gaps is a precondition for effective functioning of the state.

Cyber Security

Cyber security is defined in the National Cyber Security Strategy of the Czech Republic for the Period 2015–2020 as a concept covering:

> *"organizational, political, legal, technical, and educational measures and tools aiming to provide a secure, protected, and resilient cyber space in the Czech Republic for the benefit of both public and private sectors, as well as for the general public. Cyber security helps to identify, evaluate, and resolve cyber threats, to reduce cyber risks and to eliminate impacts of cyber attacks, cyber crime, cyber terrorism and cyber espionage by enhancing confidentiality, integrity, and availability of data, information systems and other elements of information and communication infrastructure."*[21]

In other words, in the Czech Republic cyber security is understood as a term encompassing a broad range of preventive and reactive measures intended to increase robustness and resilience of national informational infrastructure.

On the national level, the NSA was designated as a competent authority in the field of

[21] National Security Authority, National Cyber Security Centre, *National Cyber Security Strategy of the Czech Republic for the Period from 2015 to 2020*, p. 5, available at: https://www.govcert.cz/download/gov-cert/container-nodeid-1067/ncss-15-20-150216-en.pdf.

cyber security. The Czech NSA is sometimes confused with the American understanding of the NSA. However, the National Security Authority is not a security service and therefore is not bound so much by the need of secrecy; let it be towards domestic or international audience. It is more open to sharing information, which is one of the key elements for creating robust cyber security.

After becoming the national authority, the NSA has established the NCSC comprising of two integral parts - the governmental CERT and Cyber Security Policies Department. The NCSC has several key objectives. Among other things it strives to prevent and respond to cyber security incidents to minimize the harm they cause to the Czech Republic. It nurtures national cyber security capability and provides leadership on critical cyber security issues. It acts as an awareness raiser, educator and organizer of cyber exercises. It further reduces risk posed to the country by working with its international partners, with the private sector and academia.

The NSA, however, does not ensure cyber security of the Czech Republic alone. The NSA is set to protect mainly critical information infrastructure and important information systems against cyber incidents. Supervision over electronic communication service providers, natural and legal persons administrating important networks (unless being administrators of CII and IIS) is exercised by the National CERT. The National CERT is responsible for providing its constituency with methodical support in case of a cyber security incident. ISPs have a duty to report incidents to the National CERT, not to Government CERT as administrators of CII and IIS do, and in case of cyber emergency, they have to implement measures prescribed to them by the NSA. The role of the National CERT is performed by the CSIRT.CZ, which is operated by CZ.NIC - the country code top-level domain trustee and a private law association of ISPs. The CZ.NIC association operates the National CERT on the basis of a public contract with the NSA.[22]

Cyber Defence

Cyber defence, in contrast to cyber security, is understood as a concept referring to a narrower spectrum of activities. From the Czech perspective, cyber defence can be understood by an analogy with defence in the physical environment. In this sense, it is an activity focusing on protecting the state against advanced hostile attacks undermining state's integrity, sovereignty, national interests and economic well-being. Cyber attacks falling under the cyber defence concept are attacks that threaten the Czech ability to defend itself against external threats, are conducted on a massive scale and cannot be

[22] For more details on CSIRT.CZ's work, see: https://csirt.cz/page/882/o-nas/.

handled by the traditional cyber security tools and measures alone. Cyber attacks falling under the cyber defence concept are thus more focused and the state does not face them as often as it faces cyber security incidents.

Considering the nature of cyber defence, the Military Intelligence Service, a part of the Ministry of Defence, and its National Cyber Forces Centre was a natural choice for a competent national authority in the field of cyber defence. The Centre is responsible for minimizing impact of attacks such as, for example, cyber attacks used as a part of military or hybrid operations, cyber espionage directed at acquiring information of military character, or enemy's cyber campaigns aimed at achieving military goals. Cyber defence of a country, however, is no longer viewed simply from a passive and preventive point of view. Transition from the passive and preventive cyber defence to an active one and the use of the active cyber defence concept has been taking place across states in the last few years and the Czech Republic is no exception. The Military Intelligence Service has started developing capacities necessary for conducting a wide spectrum of active defence operations and other activities necessary for performing the task. The Ministry of Defence (MoD) is responsible for reducing impact of cyber attacks threating to hinder operations of the Czech Armed Forces and for ensuring security of communication and information systems and military networks. Within the MoD and the Armed Forces, the agency in charge of protection of military networks is the Communication and Information Systems Agency (CISA). It directs and provides for operational planning with regard to computer information systems, is responsible for static computer information systems on the Czech territory, and coordinates a non-public telecommunication network for the Armed Forces and MoD. Incorporated in the CISA structures is the Computer Incident Response Team (CIRC). It is in charge of protecting all MoD communication and information systems.[23] The Ministry of Defence is also responsible for cooperation with NATO and the EU in the area of planning, building and developing capabilities of the Czech Armed Forces.

Cyber Crime

Unlike cyber defence, which deals mainly with state and non-state military actors whose motivation is rather political, here perpetrators are hackers with criminal motivation. They exploit the Internet in variety of ways. Some crimes exist only in the digital world, especially those targeting the integrity of computer networks. But the Internet is also widely used as a platform for committing frauds and identity thefts and it provides

[23] Communication and Information Systems Agency, available at: http://www.army.cz/scripts/detail.php?id=87183.

opportunities for those seeking to exploit children. The nature of the cyber space allows criminals to target the Czech Republic from different corners of the globe, making it harder to enforce law. As the level of digitalization keeps increasing, so does the scope of potential victims of cyber crime. However, for a state to keep developing and its economy growing, it has to create a secure cyber space so that its population can trust in online services.

As the largest armed security force in the Czech Republic, the Police is one of the main pillars of the homeland security and its law enforcement forces play a fundamental role in the fight against cyber crime threats. Its task is to detect and investigate criminal activity. The key to performing this are professionally trained officers in the environment of social networks, in hidden parts of the Internet and identification of originators of cyber crime threats. Within the Police, the agency responsible for investigation of cyber crime is the newly established Unit for Combatting Organized Crime. Its priorities in combatting cyber crime are the fight against child pornography, property crimes on the Internet or copyright violations.

No cooperation, no effective security

Unless national authorities in the field of cyber security, defence and crime cooperate, comprehensive policies protecting the state from cyber threats cannot be developed. Unless they share information, none of them can have a complete picture of the overall situation. The Cyber Security Council is the official forum for interagency cooperation. It is a platform in which its members can coordinate cyber issues and create unified policies. The National Security Authority has also an irreplaceable role in coordinating all related activities. It leads cooperation across governmental departments, strives to increase capacities and capabilities of all of them and bridges gaps among cyber security, cyber defence and cyber crime.

Cooperation and information sharing should be further strengthened by activities of Czech intelligence agencies. Beside the already mentioned Military Intelligence Service, the Office for Foreign Information and Relations and Security Information Service collects and analyses information indicating threats to security and interests of the state, including threats in the cyber space. Their task is to contribute to cyber security by sharing the information with relevant state administration bodies.

More cooperation will also be needed at the "hybrid threats" front, which comprises many segments, including cyber. Thorough understanding of all of the aspects of hybrid warfare and cooperation across the government is needed to face this challenge effectively. Establishment of the Centre Against Terrorism and Hybrid Threats under the Ministry of Interior in the beginning of 2017 was an initial step. The centre has started to monitor a broad scope of threats, such as terrorism and disinformation campaigns, and on basis of analysis, it should propose new solutions to the problem.

Cyber security, cyber defence and cyber crime are issues that can hardly be separated. A state cannot ensure its full security by neglecting any of the three. As shown above, cyber security is an all-encompassing concept. By protecting CII and IIS, the Czech Republic ensures smooth functioning of the state. By cooperating with international partners, developing national strategies and raising awareness, it increases cyber robustness and resilience of the country. Cyber defence protects the state against serious cyber threats undermining state's integrity, sovereignty and national interests. Deterring cyber crime protects the economy and population and increases its trust in digital technologies. Cyber security, cyber defence and fight against the cyber crime create a comprehensive protection framework. Without one, protection of the whole state fails. The Czech Republic has to aim to continuously develop all segments of the three. Only through a joint effort and cooperation among all of the above-mentioned bodies will the Czech Republic be able to effectively ensure cyber security of the country and protect itself from such attacks as were those in March 2013.

Conclusion and Future Vision

Apart from the institutional and legal framework that is in place in the Czech Republic, the core element of enhancing cyber security is trust. Although the legal framework stipulates the obligations and sets forth the activities of the NCSC, trust between public and private sector and between public entities is the cornerstone of all efforts. Enhancing cyber security, deepening technical and non-technical expertise, acquiring latest technologies, adopting best practices, these are all essential. But without trust based cooperation, willingness to cooperate above the minimum required by law and people who are the bearers of trust, whole cyber security framework would be a good model, but still just a model. Therefore, human capital, despite dealing with predominantly technical challenges at the beginning, is the most important part of any cyber security efforts. As challenges emanating from cyber space become more of societal, economic and national security nature, the expertise provided constantly by the professionals across government, public, private and academic sector is the founding block of all efforts to secure the cyber space. Therefore, the Czech Republic is actively promoting forging partnerships abroad and nationally, forming alliances and cooperation platforms among likeminded entities.

Moreover, to continue its fight against modern cyber threats and boost its vision of comprehensive national cyber security, born in the aftermath of the March 2013 cyber campaign, the Czech Republic pledges to keep building and strengthening its national capability and capacity in cyber space and so to satisfy the increasing demand for NCSC's services. As a part of this commitment, the government agreed, in November 2016, to boost the NCSC capacities. By 2025, the centre should thus grow up to ten times in staff and budget and acquire new premises built between 2020–2022, which will allow for a larger range of activities as well as higher quality of services offered.

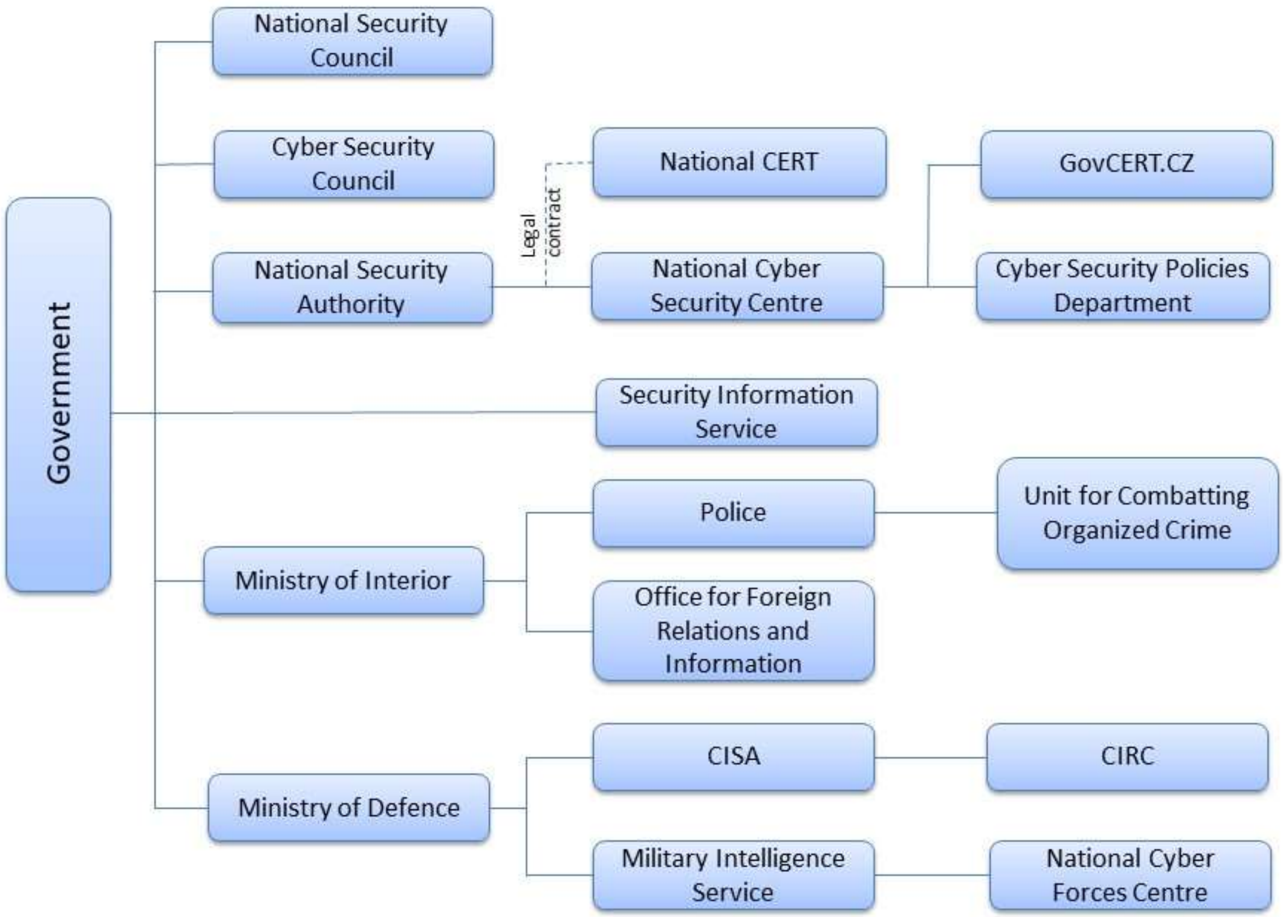
Further, in December 2016, the government decided that a truly comprehensive approach to cyber security in the Czech Republic warranted creation of a dedicated agency and decided to separate the cyber element from the NSA in order to form the National Cyber and Information Security Agency, a civilian organisation that would encompass cyber security of both unclassified and classified information systems.[24] The NIS directive transposition and related legislative amendments will thus also serve as a vehicle for creation of this new administrative body.

The new agency, operational from 1 August 2017, will take over the portfolio of cyber activities from the NSA. It will continue in protection of critical information infrastructure

[24] Resolution of the Government of the Czech Republic No, 1178 of 19 December 2016 (only in Czech), available at: https://apps.odok.cz/attachment/-/down/RCIAAGWBZE5J.

along with other entities bound by the Act on Cyber Security. The agency will also be responsible for information security in classified systems, including their certification or research and development of relevant cryptographic tools. To conclude, the Czech Republic is committed to keeping up to its resolution set in the current National Cyber Security Strategy to play leading role in the field of cyber security not only in the region but in the whole of Europe.

Annex: Graphics of the Czech organization of cyber activities before the organizational changes of 2017


Government
National Security Council
Cyber Security Council
National Security Authority
Legal contract
National CERT
National Cyber Security Centre
GovCERT.CZ
Cyber Security Policies Department
Security Information Service
Ministry of Interior
Police
Office for Foreign Relations and Information
Unit for Combatting Organized Crime
Ministry of Defence
CISA
CIRC
Military Intelligence Service
National Cyber Forces Centre

Sources

- National Security Authority, National Cyber Security Centre, *National Cyber Security Strategy of the Czech Republic for the Period from 2015 to 2020*. Available at: https://www.govcert.cz/download/gov-cert/container-nodeid-1067/ncss-15-20-150216-en.pdf.
- National Security Authority, National Cyber Security Centre, *Action Plan for the National Cyber Security Strategy of the Czech Republic for the Period from 2015 to 2020.* Available at: https://www.govcert.cz/download/gov-cert/container-nodeid-578/ap-cs-2015-2020-en.pdf.
- National Security Authority, *Strategy of the Czech Republic in the Field of Cybernetic Security for 2012–2015*. Available at: https://www.govcert.cz/download/legislativa/container-nodeid-1073/20120209strategieprooblastkbnbuen.pdf.
- National Security Authority, National Cyber Security Centre, *Report on the State of Cyber Security in the Czech Republic 2016*. Available at: https://www.govcert.cz/en/info/publications/2534-report-on-the-state-of-cyber-security-of-the-czech-republic-2016/.
- European Commission, *Digital Economy and Society Index 2017*, country profile: Czech Republic. Available at: https://ec.europa.eu/digital-single-market/scoreboard/czech-republic.
- CESNET, official website. Available at: https://www.cesnet.cz/?lang=en.
- CSIRT.CZ, official website. Available at: https://csirt.cz/page/882/o-nas/.
- Communication and Information Systems Agency, official website. Available at: http://www.army.cz/scripts/detail.php?id=87183.
- Nováček, Martin. „Právo o pátě: Radim Polčák - koordinace obrany před kybernetickými útoky je potřeba." *Pravniprostor.cz*, 2014. Available at: http://www.pravniprostor.cz/clanky/ostatni-pravo/pravo-o-pate-radim-polcak.
- Act No. 181/2014 Coll., on Cyber Security and Change of Related Acts. Available at: https://www.govcert.cz/download/legislation/container-nodeid-1122/actoncybersecuritypopsp.pdf.
- Explanatory Report of the Act on Cyber Security and Change of Related Acts. Available at: https://www.govcert.cz/download/aktuality/container-nodeid-571/nbu-zkb-navrh-140102-vlada.pdf.
- Resolution of the Government of the Czech Republic No, 1178 of 19 December 2016. Available at: https://apps.odok.cz/attachment/-/down/RCIAAGWBZE5J.