III.

Legislative Intent of The Law on Cybernetic Security

Contents

A: Final Report on evaluation of effects of regulation

1. Reason for submission

1.1 External influences

A distinctive growth in usage of information technologies in today's world leads on one hand to creation of information society, faster communication and large development of services and with that of the whole society. Dependence of functioning of society on information technologies is rapidly growing in all fields (it does not deal only with services of information society such as online shopping, but also with functioning of other information systems on whose proper functioning are dependent all sort of basic functions such as infrastructure, energy transmissions, exercise of public governance etc.) However, with growing dependence of society on information technologies is on the other hand also associated growing risk of misuse of these technologies. This has a large impact on activity of entities, which work with them and it could potentially lead to substantial damages.

General trend around the world is a high quality protection of these information technologies, preventing a misuse which could endanger their functioning. Aimed attacks against information technologies are worldwide phenomenon and their impact causes extensive economical damages in both public and private sectors and can concurrently provoke negative political incidences on national, international and even global scale. In cases where the attack is aimed against elements of critical infrastructure, the final result could endanger security or existence of the state.

Attacks against information technologies are more and more sophisticated and complex. They are shifting from the sphere of economical profit of individual attacker to organized industrial cybernetic espionage and cybernetic terrorism. Attackers continuously aim at elements of critical infrastructure, such as energetic system, pipelines and health and public governance information systems.

With regard to the fact that cyberspace has no limits and therefore is not an issue of territory, it is necessary to resolve attacks at information technology from international community's perspective and with regard to obligations of Czech Republic to North Atlantic Treaty Organization (NATO) and European Union (EU). In the framework of international regulation of this phenomenon evolves a growing pressure on Czech Republic to regulate protection of cyberspace in form of obligatory legal regulations.

Ensuring cybernetic security of the state is one of the main challenges of the present day. NATO summit in Lisbon, held in 2010, emphasized the necessity of dealing with this problem not only as an international issue but also as a national one. The pervasiveness of these limitless threats asks for intensive international cooperation as well as for intensive efforts in cybernetic security in particular states.

The issue of cybernetic security is and will be one of the determining factors of security environment in the Czech Republic. All developed countries, among which Czech Republic undoubtedly belongs, are now fully dependent on proper functioning of information and communication systems. The rise and development of competitive society based on use of advanced technologies and proper function of information society is dependent on those systems. Services of information society including related facilities and activities are one of the most dynamically developing sectors of every modern economy since many entrepreneurial entities and to a certain degree also the quality of living of all citizens is dependent on them. The security of cyberspace of every

country is becoming the evaluating criterion for investors and significantly influences competitiveness of that particular country.

We can assume that at the time when a larger part of economical activity is shifting to internet and growing percentage of Gross National Product is depending on proper functioning of technologies, investing into cybernetic security is adequate and justified expense in terms of prevention and lowering risks of frequent and extensive attacks and incidents which considerably weaken and negate economical, political, cultural and other benefits of development of the electronic sphere.

It is obvious, that not only economical activities are shifting to cyberspace. From being the best known part of cyberspace, the internet, With emergence of social networks, gaming networks and hobby networks, the internet rises from being the best known part of cyberspace to society-wide phenomenon, through which can society be affected in positive or negative terms.

1.2 *Internal influences*

The security of cyberspace is solved through private entities without any regulation by particular bodies in the Czech Republic. These bodies often solve possible attacks at information technology randomly ad hoc, without qualified recommendations from the central level. They lack findings on the past attacks and have to solve them independently, unnecessarily increasing the expenses.

There is no united system of security standards, which would minimize potential damage arising from cybernetic attacks in the area of public governance. There is also lack of prevention system and timely warning against these attacks. In association with growing digitalisation of public governance, the threat of cybernetic attacks is constantly increasing its relevance and it is absolutely necessary to adopt measures which would allow the state, in the framework of public governance, to react to this society-wide threat from its central position, similarly as it is suggested by international experience with serious attacks. Another influence is an effort to significantly increase the efficiency of public governance.

Since the state power may be used exclusively in the framework given by the law and private entities may be regulated only by law, it is necessary to regulate the area of cybernetic security by law, with detailed division of obligations of entities, which are

primarily important for the functioning of the state and other entities; by determining roles of entities affected by the public-law regulation; and unification of terms used in the sphere of cybernetic security.

Among the main risks concerning inactivity is the increase of number of cybernetic attacks, substantial material damages, endangering critical infrastructure of the state and last but not least also failure to meet international obligations of the Czech Republic, including the obligations resulting from agreements on protection of investments.

Last but not least, another internal influence is adoption of Decision of the Government of the Czech Republic, dated 19th October 2010 n. 781 regarding designation of the National Security Authority (hereinafter "NSA") as responsible for the cybernetic security as well as national authority for this area. Based on this ruling, the NSA was among other tasks assigned to establish fully functional National Centre for Cybernetic Security till the end of 2015.

1.3 Description of end-state in the field of cybernetic security

Basic aim of the Law on Cybernetic Security is to enhance the security of cyberspace, set up active cooperation mechanism between private sector and public governance to be more effective in resolving cybernetic security incidents and introduce a set of rights and obligations. By setting predictable and transparent procedure for all entities affected by the regulation, based on gradual steps that should provide detailed overview of threats and risks that exist in the cyberspace, it will guarantee the opportunity to swiftly react to new threats that will arise in the future. The legislative intent is not aimed to eliminate all risks that could affect all users of cyberspace but will try to protect the part of the infrastructure which is significant for the functioning of the state and whose disruption would lead to damage or threat to the interest of the Czech Republic. Particular obligations aimed at protection of their information systems and networks they operate, shall be prescribed to such entities. These obligations may be perceived as minimal nevertheless they still ensure reaching the anticipated goal. Recommendations will be published for the so called common users and conclusions based on best practices will be formulated.

Goals are determined in the following categories:

- Creation of rights and obligations of the state which is entrusted with authority to ensure cybernetic security in association with rights and obligations of other state bodies and private entities which operate in this field.
- Setting of mechanism of transfer of information necessary for prevention of cybernetic threats which will serve for analysis of possible cybernetic attacks and as means for its timely prevention.
- Creation of early warning system, prevention and public education including providing assistance with introduction of preventive measures and counter-measures during threatening attack.
- Standardizing configuration of security of systems necessary for functionality of the state in area of critical informational infrastructure of the state.
- Determination of rules for coordination of activities in diverting threatening attack aiming at elements of critical informational infrastructure of the state and in solving issues in which there is need to accept measures in order to prevent possible consequences of threatening attack.

The end-state of the mentioned activities is establishment and maintaining of trustworthy and competitive information society with emphasis to development of free and safe use and sharing of information and last but not least also improving the image of the state in this field, both domestically and internationally.

1.4 Description of current state and partial solutions of cybernetic security

The development of solution of national cybernetic security was subject to Governmental concept documents and initiatives of private and academic sphere. It can be summarized in the following way:

2000 – Amended Concept of Fight against Organised Crime [1)]

This document entrusted Ministry of Interior among other things also to "continuously and conceptually eliminate organised criminal activities in the area of information technologies".

2001 – Concept of fight against crime in the area of information technologies [2)]

It was adopted in line with obligations assigned to the Ministry of Interior by the Amended Concept of Fight against Organised Crime and embodied first significant document containing efforts to ensure cybernetic security. Its schedule assigns to the Department of Security Policy of the Ministry of Interior, in cooperation with Department of Communication and Information Services, Departments of Concepts, the Police Presidium and the Office of Investigation among other things:

- To provide conditions for further development (including material and personal strengthening) of structures directly involved in fighting information crime.
- Enlarge and support cooperation of police bodies with intelligence agencies and non-governmental non-profit entities, dealing with fight against certain aspects of information crime.
- To create principles of plan for protection of state and some strategically important non-state information systems.
- To create project of signalling system for crime in the area of information technologies.
- To initiate foundation and support of the CERT-type (Computer Emergency Response Team) group as non-governmental association of qualiffied experts informing other professionals about security problems and reacting to continuous attacks.
- To create project of education of law enforcement bodies with emphasis to solution of criminality in the field of information technologies (including preparation of study materials).

[1)] Decision of the Government of the Czech Republic dated 23rd October 2000 n. 1044 to the Amended Concept of Fight against Organised Crime.

[2)] Approved by the ministry of Interior on 5th July 2001

- To develop and implement forensic standards for search and evaluation of electronic data during criminal investigation and criminal proceedings.
- To support independent scientific, publication and documentary activities dealing with cybernetic incidents.
- To promote and propagate proper conduct of experts and wide public associated with fight against information criminality.
- To follow activities in international and supra-national organisations in the field of fight against crime in the area of information technologies. To actively engage in international events dealing with fight against information criminality.

2004 – State Information and Communication policy e-Czech 2006[3)]

This document was approved in association with expected entry of the Czech Republic to the European Union. It was aimed to define "main principles to be implemented by the Government during further development of information society in the Czech Republic". Among others, it stated four areas of priority in state information and communication policy while one of them were available and secure communication services. In the area of security of electronic communications, the Government took the aim to actively support ensuring security of state communication infrastructure and specify in obligatory way parameters of those security measures which are based on law. This document provided basis for further strategic documents dealing with information systems in the Czech Republic to enforce information security in the field of communication and information infrastructure of the Czech Republic in line with section 4 para. 1 letter b) of law n. 365/2000 Coll., On Information Systems of Public Governance.

2005 – National Strategy of Information Security of the Czech Republic[4)]

National Strategy of Information Security of The Czech Republic stated tasks in the field of creation of reliable information and communication systems in the Czech

[3)] Drafted by the Ministry of Informatics and adopted by the Decision of the Government dated 24th March 2004, n. 265.

Republic. The aims of this strategy are among others "improving of management of information security and risk management", "development of knowledge about information security", support to national and international cooperation in the field of information security". Following measures were prescribed to reach those goals:

- Implementation of best practices to information security management systems.
- Continuous monitoring of threats.
- Creation of system of early warning and reaction (task to establish national centre for management, monitoring and analysis of security environment of communication and information systems in the Czech Republic is part of this measure).
- Monitoring of effectiveness of proposed counter-measures.
- Improving information security of public governance bodies.
- Protection of critical information infrastructure of the state.
- Increase awareness about information security, security risks and means of protection for citizens, commercial and non-commercial entities and public governance bodies.
- To introduce education and training programmes.
- To support general programme of national awareness about information security.
- To increase effectiveness of education programmes.
- To increase awareness of users about importance of using security certified products and services in the sphere of information and communication technologies.
- Effective cooperation and coordination on national level.
- Active international cooperation.
- Improving cooperation in national defence against information threats.

This document is followed by Action Plan of Measures and Tasks prescribed by the National Strategy of Information Security of the Czech Republic and draft Governmental

Regulation for implementation of tasks stated by National Strategy of Information Security of the Czech Republic by the bodies of public governance and critical infrastructure entities.

Concurrently the Decision of the Government of the Czech Republic dated 16th November 2005 n. 1466, on National Action Plan of Fight against Terrorism (amended version for 2005 till 2007) in the chapter dealing with cybernetic security defines task to create complex document mapping issue of cybernetic threats from the point of view of interests of the Czech Republic.

2007 – Action Plan for implementation of the National Strategy of Information Security of the Czech Republic[5)]

This document follows up to the National Strategy of Information Security of the Czech Republic and defines tasks to ensure information security in the Czech Republic. Among others, the following measures were mentioned:

- Establishment of system of early warning and reaction. To create national centre for management, monitoring and analysis of security environment of information and communication systems of the Czech Republic. Establishment of CERT-type facility with nation-wide responsibility.
- Active international cooperation. To engage in creating national and international monitoring and warning networks, able to detect and prevent electronic attacks as they emerge. Ensuring said tasks by establishment of CERT-type facility with nation-wide responsibility.

2010 – Establishment of Inter-ministerial Coordination Council for the area of cybernetic security [6)]

The Government of the Czech Republic adopted decision n. 205, On the issues of cybernetic security of the Czech Republic, on 15th March 2010. Ministry of Interior was appointed as responsible for cybernetic security and national authority in this field.

5) Decision of the Government of the Czech Republic n. 677 dated 18th July 2007, on *Action Plan for implementing the National Strategy of Information Security of the Czech Republic*

6) Decision of the Government of the Czech Republic n. 380 dated 24th May 2010, on establishment of *Inter-ministerial Coordination Council for the area of cybernetic security*

Ministry of Interior was entrusted with task to create Inter-ministerial Coordination Council for the area of cybernetic security.

The Council was supposed to be main coordination body in the field of cybernetic security in the Czech Republic, while its main goal was the support of administrative and coordination role of the Ministry of Interior. The Council had primarily the following tasks:

- to coordinate activities of state bodies in the field of cybernetic security and contribute to implementation of tasks of inter-ministerial nature,
- to coordinate state bodies while fulfilling tasks in the field of cybernetic security, stemming from the membership of the Czech Republic in the international organisations and coordinate representation of the Czech Republic in international organisations and international activities associated with cybernetic security,
- to demand necessary level of participation from the bodies represented in the Council while fulfilling tasks in the field of cybernetic security,
- to actively create conditions for smooth cooperation among its members,
- to solve current issues of cybernetic security and to present expert drafts and recommendations to the Minister of Interior and to the Government via him if needed,
- to monitor fulfilment of conclusions of the Council by its members,
- to collect, analyze and evaluate data provided by its members on the state of cybernetic security,
- to prepare draft reports on the state of cybernetic security in the Czech Republic, which was to be presented by the Minister of Interior to the Government on a regular basis as a document stating priorities and tasks stemming from them for the following period,
- to cooperate with external expert entities and use their inputs in order to ensure cybernetic security of the Czech Republic.

The Inter-ministerial Coordination Council for the area of Cybernetic Security was dissolved after the transfer of responsibility over cybernetic security to the NSA by the Decision of the Government of the Czech Republic n. 781 dated 19th October 2011.

2010 – Signature of Memorandum on Computer Security Incident Response Team (CSIRT) of the Czech Republic with the CZ.NIC Association[7)]

There are several established and informal CSIRT/CERT type teams. They have experience with attacks, they share information and were incorporated into international structures. These teams cooperate in the framework of the CSIRT.CZ working group coordinated by the CZ.NIC Association. An agreement between the Ministry of Interior and CZ.NIC Association that the Association will take over the responsibilities of the National Computer Security Incident Response Team of the Czech Republic (CSIRT.CZ) was reached by signing the Memorandum on Computer Security Incident Response Team (CSIRT) of the Czech Republic. CSIRT.CZ should contribute to solve incidents in the field of cybernetic security in the networks operated in the Czech Republic, to provide assistance to the end-users, to collect and evaluate data on reported incidents, to act as Point of Contact in the field of IT and educate public in cybernetic security. Cooperation with other CERT teams on national and international level is expected. This team acts till 30th July 2012 also as Governmental CERT of the Czech Republic.

2011 – Strategy in the field of cybernetic security of the Czech Republic for 2011 – 2015 [8)]

Strategy in the field of cybernetic security of the Czech Republic for 2011 – 2015 follows up to the Security strategy of the Czech Republic and defines intentions of the Czech Republic in the field of cybernetic security. It aims primarily to protection against threats against information and communication systems and mediation of damages

7) As agreed on 9th December 2010 by the Ministry of Interior and CZ.NIC, z.s.p.o. https://www.csirt.cz/files/nic/doc/Memorandum_CZ.NIC-MVCR.pdf.

8) Decision of the Government of the Czech Republic dated 20th July 2011 n. 564 on Strategy in the Field of Cybernetic Security 2011-2015

caused by attacks on these systems. This aim should be reached by the following measures:

- Creation of legislative framework determining the responsibilities of particular bodies during coordination of activities of public governance in the field of cybernetic security. The legislative tools should ensure cybernetic security while respecting rights granted by the Constitution to ensure prevention, reaction detection and measures aimed at fight against cybernetic crime. Also creation of rules for cooperation with the private sector is expected.
- To strengthen cybernetic security of the critical infrastructure and in information systems of the public governance, namely by defining security norms, their implementation and its supervision. Security norms should be defined in methodical documents.
- Establishment of Governmental CERT as a part of national and international early warning system. Governmental CERT should monitor and detect security incidents, react on them and act preventively to limit impact of the attacks.
- To support international cooperation in the field of cybernetic security, particularly by sharing information and experience in the framework of international organisations and strengthening cooperation with foreign entities.
- Cooperation of state, private and academic spheres.
- Raising awareness about cybernetic security.

The Action Plan divided into particular areas was adopted concurrently with the Strategy. Each area contains tasks to fulfil strategic goals of the Strategy by projects and tasks of public governance bodies responsible for that particular area.

2011 – Transfer of authority over cybernetic security to the NSA and establishment of the Council for Cybernetic Security[9)]

The NSA has become the national authority and body responsible for administration of the field of cybernetic security since October 2011. The Government has assigned to

[9)] Decision of the Government of the Czech Republic n 781 dated 19th October 2011 on designation of the National Security Authority as responsible for cybernetic security and national authority in this area.

the NSA to establish fully functional National Centre for Cybernetic Security till 2015 and as a part of it governmental coordination centre for rapid reaction to computer incidents (governmental CERT).

The Inter-ministerial Coordination Council for the area of cybernetic security was disbanded and the Council for Cybernetic Security has been established. The new Council is advisory body of the Prime Minister in the field of cybernetic security. It aims to support administrative and coordination role of the NSA in the area of cybernetic security. The membership is comprised of representatives of state bodies (Ministry of Interior, Ministry of Defence, Ministry of Foreign Affairs, Ministry of Finance, Ministry of Industry and Trade, Ministry of Transport, Police, Office for Foreign Relations and Information, Security Information Service, Military Intelligence, Office for Protection of Personal Data and Czech Telecommunication Office.

As can be seen, many conceptual and strategic documents were created in the field of cybernetic security. Nevertheless, most of their goals remain unfulfilled. However, there are practical experiences with the cybernetic security in the Czech Republic, particularly in the private and academic sphere. CERT-type teams, working on academic and private basis have the most experience with resolving of cybernetic security incidents. Currently, there are five teams officially recognised by the international infrastructure of the CERT teams:

- CESNET-CERTS
- CSIRT.CZ
- CZ.NIC-CSIRT
- CSIRT-MU
- ACTIVE 24-CSIRT.

Czech pioneer in this field is association CESNET z.s.p.o., founded by Czech universities and the Academy of Sciences in 1996. Its main task is development and operating of backbone academic network of the Czech Republic. Current version of this network is called CESNET2 and is used for scientific, research, development and educational purposes. Sub-networks of its members, some high schools, hospitals and libraries are connected to this network. Security in the network is supervised by team

CESNET-CERTS[10], established in January 2004. This team is directly responsible for resolution of security incidents of hardware and services in the CESNET2 network, it maintains problem-free operation of the network and prevention of security incidents. It also supports members of the association and system administrators of the connected networks in creation of their own security strategies. Besides its main activity CESNET-CERTS also carries out educational activities in the form of training courses for representatives of its members and is engaged in international cooperation with other CERT teams. Security teams of particular members are also active in the CESNET2 network playing the role of local CERTs:

- CSIRT team of computer network of VŠB-TU[11] (University of Mining) Ostrava, founded in 2008 solves security incidents in VŠB-TU Ostrava.
- CSIRT-MU[12], was established in 2009 at the Institute of IT of Masaryk University in Brno. Its main goal is solving security incidents in the university network. CSIRT-MU is listed in the official list European CSIRTs.
- CSIRT-VUT[13] is responsible for solving security incidents in computer network of the Technical University in Brno.
- ACTIVE 24-CSIRT solves all incidents in the network of its company and coordinates with other security teams in the Czech Republic.
- WIRT[14] (WEBnet incident response team) investigates and solves complaints and reporting of security incidents in the network of West-Bohemian University in Plzeň.

CIRC MO centre is the body of cybernetic security at the Ministry of Defence. Its task is active identification of security threats, their analysis and following reporting of found incidents and procedures for their solution to the relevant partners. CIRC MO centre helps to protect information and data stored in the information systems and technical means of command and communication in the framework of Ministry of Defence.

[10] https://csirt.cesnet.cz/.

[11] http://idoc.vsb.cz/cs/okruhy/cit/tuonet/info/csirt/index.html.

[12] http://www.muni.cz/ics/services/csirt.

[13] http://www.vutbr.cz/cvis/sit/csirt.

[14] http://support.zcu.cz/index.php/WIRT_-_WEBnet_Incident_Response_Team.

Another key CERT-type team is the security team of CZ.NIC Association. CZ.NIC, z.s.p.o. is association established in 1998 by the most important internet service providers (it has currently 94 members). Main activity of the Association is running the national register of ".cz" domain names, ensuring operation of the TLD and education in the field of domain names. Its CZ.NIC-CSIRT team is responsible for solving security incidents in its own network and incidents involving ".cz" domain name servers. The specific feature of this team as the team of national domain administrator is capability to deactivate particular domain which is source of incident of national or international importance. Such incident may be for example spreading malicious content, pretending of content of other service (phishing) or hardware connected through domain distributing malicious content (p.e. botnet).

The pilot project of CSIRT.CZ[15)] was started in 2008. It was operated at the beginning by CESNET-CERTS team and its main task was coordination and assistance to users during security incidents originating or aimed at networks in the Czech Republic and which were not solved by the administrators of the networks themselves. In this way CSIRT.CZ operated as a team of "last hope" for security attacks at Czech networks and thus played the role of National CERT team. This project was finished at the end of 2010 and since then the CSIRT.CZ acts as official National CERT team operated by CZ.NIC Association. Its main tasks are:

- Maintaining international relations with the world community of CERT/CSIRT teams and organisations supporting this community.
- Cooperation with entities in the Czech Republic, ISPs, content providers, banks, security structures, academic sector, state bodies and others.
- Providing services in the field of security:
    - Resolving and coordination of resolving security incidents.
    - Education and training activity.
    - Active services in the area of security.

[15)] http://www.csirt.cz/.

CSIRT.CZ also cooperates with foreign subjects; first of all international organisations ENISA[16)], TERENA[17)] a FIRST[18)].

The Memorandum of Understanding between NSA and NATO Cyber Defence Management Board – CDMB) on cooperation in the field of cyber defence has been signed on 14th March 2012.

2. Proposed alternative solutions

The alternatives of regulatory model have to be based on the following premise:

It is necessary to process data about cybernetic security incidents from the widest range of sources possible to ensure cybernetic security and corresponding right for information self determination through access to functioning services of information society. That is because large scale cybernetic attacks may be considered as minor incidents in local networks. Only monitoring of larger part of information or communication infrastructure may in such cases bring adequate identification of cybernetic attack, its scope and the danger it poses. The protection measures have to be coordinated for the same reason. That is because services of information society are distinguished by their network character while even a small component of the network may significantly influence its other parts often regardless geographic proximity.

2.1 "Zero alternative" (without specific regulation)

As zero alternative may be considered as continuing of the current state – non-existence of specific legal regulation and no central public governance body responsible for cybernetic security. Ensuring of cybernetic security is in such situation dependent on voluntary coordination of supervisory and protection activities among particular providers of electronic communication services or entities responsible for operation of electronic communication networks. It is to be noted that even relatively insignificant

16) European Network and Information Security Agency zdroj: http: //www.enisa.europa.eu/.

17) Trans European Research and Education Network Association. This organisation acts as forum for cooperation, innovation and knowledge sharing aimed at development of internet technologies, infrastructure and services for research and academic community. Source: http://www.terena.org/.

18) Forum for Incident Response and Security Teams. FIRST groups different CERT teams from state, private and academic organisations. Aim of this association is cooperation and coordination in resolution of security incidents – source: http://www.first.org/.

provider of services or entity operating network may by its unwillingness to cooperate on a system of cybernetic security provide enough space to the attacker to seriously threaten the cybernetic security.

From the point of view of security, the zero alternative would bring a large degree of risk followed by absence of effective tools for protection against cybernetic attack of society-wide nature. From the economic point of view, the zero alternative seemingly saves direct investments to establish and maintain national cybernetic security measures. It would also save investments of private entities and public governance bodies to secure their systems (to install mandatory security measures). However, at the same time it would lead to significant rise of costs to secure particular systems when decided by the operator. Both private and public entities interested to secure their systems (entities with strong economic or political interest in security of their systems) would be forced to invest disproportionately more money into their infrastructure than they would have to if the law stated basic security standard and set appropriate institutional background.

The case is the same as fire fighting. If there is no basic standard and institutional background, the entity interested in own protection has to invest not only to its own means but also to means protecting against fire from unsafe neighbouring buildings. In the end it would be neither economical nor effective, bringing increased pressure on other means of protection.

Some of the particular measures in reaction to the raising amount of cybernetic attacks were already adopted by private and public institutions and their costliness already promoted limited cooperation and centralisation of the CERT / CSIRT teams.

From the philosophical point of view, the zero alternative would mean resignation of the state to protection of one of the fundamental rights whose importance is raising constantly – the right for informational self-determination. Indirectly it would mean also resignation of the state to protection of ownership (ownership of information and communication infrastructure) and to the responsibility of the state to foreign investors in the ICT sector. Therefore, the current state is intolerable due to necessity to fulfil international obligations.

The only situation when the zero alternative could be effectively implemented is the case of decrease of number and dangerousness of cybernetic attacks. Since the trend is

quite the opposite, the zero alternative is totally unfit. The current trends also confirm that the zero alternative retreats to the more progressive options mentioned below.

2.2 Alternative of protection of information systems processing classified information

This alternative is based on assumption that the regulation shall be aimed only to networks dealing with classified information. The protection of relatively small part of information and communication infrastructure would bring only a small need of investments also bearing in mind that the protection of classified information is adequately handled by special legal regulation.

The classified information present only one of many critical parts of the information society. With its development and move of significant part of social life into the sphere of information technologies also other functions are of critical importance. Not the classified information but other services, including significant part of political and economic activity, embody the crucial part of one's right for informational self-determination.

The concept of cybernetic security limited to classified information would therefore be only partial and would not fulfil its function. The legal regulation would in such case cover the issue of cybernetic security on national level but there would be no means for effective protection of services fundamentally important for the functioning of the state, society and every citizen.

2.3 Alternative of general authority over public governance bodies

This alternative could not be implemented for the following reasons. Information systems of public governance and their communication infrastructure present only part of information systems and services of electronic communications necessary for the functioning of the society. Without including private entities, the solution would be only partial, able to react only to attacks against public governance information systems but not to attacks against other information systems initiated by security incident in the public governance network. This alternative would not bring compliance with the obligations to allied nations of NATO and EU.

2.4 Alternative of general authority with cooperation with private entities

This alternative is based on the principle of generality. It includes various information systems, networks and services of electronic communications shaping the Czech cyberspace whose security has direct influence on the security of the state.

This alternative is also based on presumption that private entities are owners of significant part of the information infrastructure of the state, including the one with critical importance. The information services important for both state and private sector are provided by private entities on commercial basis.

The security of the Czech cyberspace is crucially important for those private entities because only the functioning network can generate proper economic effect. These private entities invest in securing their own infrastructure and are economically motivated to participate on protection of overall cybernetic security.

The alternative of cooperation with private entities is also based on presumption that these entities are technically and legally most suited to resolve cybernetic security incidents in their own infrastructure. That is possible due to detailed knowledge of their own systems, direct technical control and also legal relations. Information and communication systems are either directly owned or legally or effectively controlled by the relevant entity. The state can never reach the same rights while respecting the Constitution at the same time.

It can be presumed that the new burden and other costs will be appropriate to the relation to the protected interest and their investment will be more effective in comparison with the zero option. The commercial entities will have more secure environment for their business. The obligatory nature of the legal regulation ensuring same level of security standards shall be implemented only in the case of critical infrastructure.

This option seems to be ideal for ensuring cybernetic security in the Czech Republic due its constitutional conformity, high effectiveness and low costs.

2.5 Alternative of general authority and direct regulation

This alternative is based on assumption that the state directly controls and regulates functioning of the information society through its bodies. It requires creation of

competences for the designated state authority (NSA) to directly implement security and protective measures. It would require establishing NSA powers over the users which would directly harm their right for informational self-determination. It would be also necessary to affect ownership and other rights of entities providing services or operating information networks to allow NSA to directly influence functioning of electronic communication networks and services.

Besides the regulatory burden bestowed upon the private entities, the direct regulation option is also very demanding from the technical and organisational point of view. The NSA technicians would have to manage a large number of communication systems with installed probes or devices allowing their direct control. The direct regulation is most demanding as regards direct costs and personnel compared to other options.

Due to its extreme economic and organisational demands and problems with constitutional conformity this alternative seems to be inappropriate and unworkable.

2.6 Evaluation of costs and benefits

The issues to be regulated are widespread across various entities and areas. The proposed solution is based on foreign experience while respecting the long term government strategy in the field of cybernetic security. The new regulation will bring substantial rise of security of information society. Central system of monitoring of cybernetic attacks, early warning and counter-measures systems will lead to better prevention and to better effectiveness of public governance and entrepreneurship. The costs to remove the consequences of cyber-attack are individual because they include not only damages caused by the incident itself but also losses (p.e. in the financial or security spheres).

For this reasons it is hard to evaluate concrete costs and benefits for particular groups. Therefore, the evaluation focuses on general evaluation of costs and benefits of proposed alternatives, fist of all from the point of view of reaching the stated goal.

Quantitative evaluation of costs and benefits is very complicated at the current phase as is evaluation of actives endangered by attack. The proposed alternatives are

evaluated from the point of view of particular groups as well as general benefit for the legal environment in the Czech Republic in the field of cybernetic security.

At this stage, only the costs necessary to establish and operate the National Centre of Cybernetic Security may be quantified. The Decision of the Government n. 781 dated 19th October 2011 provides for continual rise of personnel. That is rise of 8 positions in 2012, 10 positions in 2013, 10 positions in 2014 and 5 positions in 2015 with the associated rise of NSA budget for 51.5 mil. CZK in 2012, for 61 mil. CZK in 2013, for 61 mil. CZK in 2014 and for 65 mil. CZK in 2015. There may be rise of relevant positions required at the Czech Telecommunication Office (hereinafter "CTO") as well due to its new responsibilities.

3. Determination of groups and areas affected by regulation

3.1 Personal and material authority

The law is intended to affect so called definition authorities of the Czech cyberspace i.e. service providers and communication network operators as well as administrators of selected information systems (those included in the critical information infrastructure and information systems of the public governance).

The law is based on functional model – it distinguishes the entities not on the basis of their nature but according to their function in Czech cyberspace.

The law distinguishes the following groups of affected entities:

- Electronic communication service providers and administrators of electronic communication networks.
- Administrators of systems of communication infrastructure included in critical information infrastructure.
- Administrators of information systems included in critical information infrastructure.
- Administrators of information systems of public governance.

The law does not affect directly the users of services and communication networks. That is important feature in order to preserve right for informational self-determination which is associated with basic human rights as ownership and freedom of speech.

The material authority of the law covers relations stemming from the obligation to implement security measures to protect the Czech cyberspace. The material authority can be generally divided into the issues of reporting and elimination of cybernetic security incidents in the networks and services of electronic communications, the issues of extent of protection of information systems of high importance (information systems included in critical information infrastructure and selected information systems of public governance) and the issues of counter-measures against the cybernetic attack.

On the other hand the law does not cover the content of services of information society and does not interfere with the right to informational self-determination. Certain limitation of services may occur in the state of cybernetic emergency.

3.2 Derogation and amendment of other legal regulations

Bearing in mind the specific nature of material authority of the law on cybernetic security, there is no significant impact on other parts of the legal system.

- Section 98 of law n. 127/2005 Coll., On electronic communications shall be amended to allow imposing sanctions to the service providers and entities operating electronic communication networks by the CTO in case of noncompliance with the requirements.
- Law n. 365/2000 Sb., On information systems of the public governance shall be amended to strengthen requirements to the security of information systems while maintaining the authority of the Ministry of Interior over administrators and operators of such systems. The authority of the NSA and Ministry of Interior over the information systems of the public governance included in critical information infrastructure shall not overlap.
- The law n. 240/2000 Sb., On crisis management (Crisis Law) shall be amended by including NSA competences of the NSA in the field of cybernetic security should the law on cybernetic security require that. Minimal level of security measures of the critical infrastructure entities shall be stated in the Law on cybernetic security or its implementing regulations. The Regulation of the Government n. 432/2010 Coll., on criteria for determination of the critical infrastructure entity shall be amended by new general criteria (including time considerations etc.). These new general criteria shall be in line with requirements for determination

of critical infrastructure entities and shall be applicable to all fields including cybernetic security. The sector criteria shall be also amended to include cybernetic security into sector „VI. COMMUNICATION AND INFORMATION SYSTEMS“. The responsible authority for the newly created sub-sector shall be NSA which will be responsible for determination of critical infrastructure in the sector COMMUNICATION AND INFORMATION SYSTEMS - cybernetic security.

- The necessity to amend other laws may emerge during the creation of the draft law itself. Nevertheless such amendments should not be substantial.

3.3 Current legislation and other documents in the field of cybernetic security

Constitutional system of the Czech Republic:

- Constitutional law n. 1/1993 Coll., Constitution of the Czech Republic,
- Charter of Fundamental Rights and Freedoms,
- Constitutional law n.. 110/1998 Coll., On the security of the Czech Republic.

Laws:

- Law n. 101/2000 Coll., On protection of personal data and amendment of other laws, as amended,
- Law n. 240/2000 Coll., On crisis management and amendment of other laws, as amended,
- Law n. 365/2000 Coll., On information systems of public governance, as amended,
- Law n. 127/2005 Coll., On electronic communications, as amended,
- Law n. 412/2005 Coll., On protection of classified information and security Eligibility, as amended,
- Law n. 69/2006 Coll., On implementation of international sanctions, as amended,
- Law n. 40/2009 Coll., Penal Code, as amended,
- Law n. 111/2009 Coll., On basic registers, as amended,
- Law n. 419/2011 Coll., On criminal responsibility of legal persons and procedures against them.

Implementing regulations

- Regulation of the Government n. 522/2005 Coll., Stating lists of classified information as amended by Regulation of the Government n. 240/2008 Coll.,
- Ordinance n. 523/2005 Coll., On security of information and communication systems and other electronic devices dealing with classified information as mended by Ordinance n. 453/2011 Coll.
- Ordinance n. 529/2006 Coll., On requirements to the structure and content of information conception and operational documentation and on requirements on security and quality management of information systems of public governance (Ordinance on Long – Term Management of Information Systems of Public Governance).

Decisions of the Government

- Decision of the Government dated 18th June 2007 n. 677 on Action Plan for implementing the National Strategy of Information Security of the Czech Republic,
- Decision of the Government dated 20th July 2011 n. 564 on Strategy in the Field of Cybernetic Security 2011-2015,
- Decision of the Government dated 19th October 2011 n. 781 on establishment of the National Security Authority as administrator of cybernetic security and national authority in this area.

Primary EU law:

- Charter of Fundamental Rights of the European Union.

Directives of the European Parliament and of the Council:

- Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations, as amended by Directive 98/48/ES,

- Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity,
- Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')
- Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services (Authorisation Directive), as amended by Directive 2009/140/ES,
- Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), As amended by Directive 2009/140/ES,
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications),
- Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks,
- Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

Regulations of the European Parliament and the Council:

- Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency,

- Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice.

Decisions of the Council:

- 92/242/EEC: Council Decision of 31 March 1992 in the field of security of information systems,
- 2011/292/EU: Council Decision of 31 March 2011 on the security rules for protecting EU classified information.

Other legislation of the EU:

- COM/2000/890 Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime,
- COM /2001/298 Network and Information Security: Proposal for A European Policy Approach,
- COM/2006/251 A strategy for a Secure Information Society - "Dialogue, partnership and empowerment",
- COM /2006/688 on fighting spam, spyware and malicious software,
- COM /2007/267 Towards a general policy on the fight against cyber crime,
- COM /2009/149 on Critical Information Infrastructure Protection - "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience",
- COM /2010/245 Digital Agenda for Europe,
- COM /2010/673 The EU Internal Security Strategy in Action: Five steps towards a more secure Europe,
- COM/2011/163 on Critical Information Infrastructure Protection 'Achievements and next steps: towards global cyber-security'.
- 2002/465/JHA on joint investigation teams,

- 2002/C 43/02 on a common approach and specific actions in the area of network and information security,
- 2003/C48/01 on a European approach towards a culture of network and information security,
- 2005/222/SVV on Attacks against Information Systems,
- 2009/C62/05 on Common working strategy in the field of fight against computer crime,
- 2009/C321/01 on a collaborative European approach to Network and Information Security,

Documents of the Council of Europe:

- Convention of the Council of Europe n. 185 Convention on Cybercrime,
- Convention of the Council of Europe n. 196 Council of Europe Convention on the Prevention of Terrorism,
- Recommendation of the Parliament Assembly n. 1706 (2005) Media and terrorism
- Recommendation of the Parliament Assembly n.1565 (2007) How to prevent cybercrime against state institutions in member and observer states?,
- Recommendation of the Committee of Ministers CM/Rec(2011)8E dated 21st September 2011 on the protection and promotion of the universality, integrity and openness of the Internet,
- Recommendation of the Committee of Ministers CM/Rec(2008)6E dated 26th March 2008 on measures to promote the respect for freedom of expression and information with regard to Internet filters,
- Recommendation of the Committee of Ministers Rec(2001)8E dated 5th September 2011 on self-regulation concerning cyber content (self-regulation and user protection against illegal or harmful content on new communications and information services),
- Recommendation of the Committee of Ministers Rec(95)13E dated 11th September 1995 Concerning problems of criminal procedural law connected with information technology,

- Declaration by the Committee of Ministers Decl-21.09.2011_2E dated 21st September 2011 on Internet governance principles,
- Declaration by the Committee of Ministers Decl-28.05.2003E dated 28th May 2003 on freedom of communication on the Internet,
- Recommendation of the General Assembly 1670 (2004) Internet and Law,
- Declaration by the Committee of Ministers Decl-07.12.2011_2E dated 7th December 2011 on the protection of freedom of expression and freedom of assembly and association with regard to privately operated Internet platforms and online service providers.

Other documents of international organisations:

- Action Plan of the European Union for fight against Terrorism (INI/2004/2214); European Parliament,
- Security of Information Systems and Networks: Towards the culture of security; OSCE,
- Report of the Special Rapporteur on support and protection of the freedom of speech n. A/HRC/17/27; OSN,
- Decision of the Council of Ministers of OSCE n. 3/2004 On fight against use of internet for the purposes of terrorism dated 7th December 2004,
- Action plan of G8 countries for fighting high-tech crime.

4. Cybernetic security abroad (not translated)

5. Implementation, enforcement and evaluation of efficiency of the regulation

5.1 Implementation

Bearing in mind the specific nature of the subject of regulation, the separate law is considered to be the best option. The specifics of the subject do not suggest to be regulated by the amendment of the Law on protection of classified information. The Law on cybernetic security may adopt some of the terminology used in other laws but has to

define also its own terms and regulate obligations of newly defined categories of entities (administrators of information and communication systems included in the critical infrastructure). With regard to the goal of the regulation it cannot be included in other law.

Bearing in mind the nature of the NSA, the new law also has to regulate specific competences of the NSA as central authority responsible for cybernetic security, including decision-making, oversight and imposing of sanctions and to determine the relation of the NSA to other public governance bodies. The specific competences of the NSA shall not include cases of committed crime. In such a case, other laws (namely the Penal code), shall be used. It is also necessary to provide for ability of the NSA to cooperate with private and foreign entities as well as work in the field of education and methodology as far as cybernetic security is concerned.

The law intends to introduce special state of cybernetic emergency to be used in case of large-scale cybernetic attack seriously endangering or disturbing security of the Czech Republic. This state shall not be regulated by the Crisis law since it does cover only entities already included in the Law on cybernetic security and has no general personal and material authority.

Due to the aforementioned reasons the model of special law has been chosen to apply. The draft law shall be prepared in cooperation of NSA and other public governance bodies dealing with electronic communications, security and crisis management.

5.2 Enforcement

The law indents to impose obligations to both private and public entities. The basic division is made on the basis of infrastructure which the particular entity administers or operates. Supervisory and sanction mechanisms are divided in a way to comply with current competences of the CSO in the field of electronic communications:

- Obligation of electronic communication service providers and administrators of electronic communication networks to report contact details for information sharing and obligation of selected electronic communication service providers and selected administrators of electronic communication networks to report

selected cybernetic security incidents – supervised and sanctioned by the CTO. Obligation of all electronic communication service providers and administrators of electronic communication networks to implement counter-measures ordered by the NSA in the case of state of cybernetic emergency – supervised and sanctioned by the NSA.

- Obligation of administrators of electronic communication networks included in critical information infrastructure to report contact details for information sharing purposes and to report selected cybernetic security incidents related to communication infrastructure included in critical information infrastructure – supervised and sanctioned by the CTO. Obligation to protect communication systems included in critical information infrastructure by security measures – supervised and sanctioned by the NSA. Obligation to implement counter-measures ordered by the NSA – supervised and sanctioned by the NSA.
- Obligation of administrators of information systems included in critical information infrastructure to report contact details for the purposes of information sharing, to report selected cybernetic security incidents related to information systems of critical information infrastructure and implement counter-measures ordered by the NSA – supervised and sanctioned by the NSA. Obligation to protect information systems included in the critical information infrastructure by security measures – supervised and sanctioned by the NSA.
- Obligation of administrators of information systems of public governance to report contact details for the purposes of information sharing and to implement counter-measures ordered by the NSA – supervised and sanctioned by the NSA. Obligation of selected administrators of information systems of public governance to report selected cybernetic security incidents – supervised and sanctioned by the NSA. Obligation to protect selected information systems of the public governance by security measures (lower standard than administrators of information systems included in critical information infrastructure) – supervised and sanctioned by the Ministry of Interior.

Supervisory competences shall be regulated in respect to the Law on state supervision. The sanctions shall include remedy measures and fines.

5.3 Evaluation of effectiveness of regulation

The intent of the new legislation itself is based on requirements stemming from the need of praxis. Also the evaluation of effectiveness of the new Law on cybernetic security, should it be adopted, shall be based on the results of supervision and consultations with entities dealing with cybernetic security. The implementation of adopted procedural rules in praxis shall be evaluated as well. As a result, the amendment or revoking of provisions not validated by praxis and introduction of new mechanisms for better effectiveness shall be considered.

6. Consultations

6.1 History of consultations

Based on the Decision of the Government n. 781 dated 19 October 2011, the NSA has been appointed national authority in the field of cybernetic security. The NSA is fully aware of indispensable role of expert public during the drafting process of the new legislation in the field of cybernetic security.

The consultations with the academic sphere were initiated immediately after the transfer of authority over cybernetic security. Working group comprised of representatives of NSA and Masaryk University Brno (IT Institute and Faculty of law – Institute of Law and Technology) has been established in November 2011. Its main task was mapping of legal framework in the field of cybernetic security in the Czech Republic and abroad. Another task was determining goals to be reached by legal regulation of the cyberspace and methods to reach those goals. The basic pillars and principles of the new legislation were agreed consensually.

Basic principles:

1) Minimal impact to the rights of private entities.

2) Individual responsibility for security of own network.

3) Respecting and strengthening of right to informational self-determination.

Three pillars of the regulation:

1) Obligation to report contact details and cybernetic security incidents.

2) Obligation to implement security measures by entities of critical information infrastructure and critical communication infrastructure.

3) System of counter-measures of cybernetic protection.

Because of the specific nature of cyberspace a special solution (independent on Crisis Law) has been chosen for determination of critical information and communication infrastructure due to inconvenient nature of criteria and already established elements of critical infrastructure stated by the Crisis Law. Note: This solution was later abandoned as can be seen below.

In parallel to this working group a platform for cooperation between NSA, MoD, Security Information Service and Ministry of Interior has been created by the Decision of the Government n. 781 dated 19th October 2011. This platform discussed above all particular aspects of the proposed regulation with the regard to its impact to the public sphere.

The need for transparent categorization of information systems of the public governance, proper legal definitions in the stage of legislative intent of the law and precise cooperation on national and international level emerged based on several consultations.

The association of legal persons CZ.NIC, operating the National CERT since 1st January 2011 was addressed as regards to the evaluation of the proposed solution to the private sector. The evaluation brought the following results:

– even lesser regulation of the private sector could be used as solution,

- state of cybernetic emergency should be declared by the Prime Minister, not the Director of NSA, due to excessive concentration of powers,

- alternative of division of powers was proposed. The Law on cybernetic security should only general framework, define basic terms and regulate only Governmental CERT and its powers over “state” networks and information systems and networks and systems included in the critical infrastructure during the state of cybernetic emergency in detail. The operation of the National CERT would not fall under NSA regulation and should be based on mutual agreements.

- necessity to tackle the problem of compensation for damages,

- necessity of broader definitions of terms,

- reduction of obligations imposed to entities under the supervision of National CERT,

- protection of personal data that may be included in cybernetic incident reports.

On the basis of these conclusions, the NSA adjusted the chosen solution. Proposal to reduce obligations of private entities was accepted – only selected electronic communication service providers and selected administrators of electronic communication networks will be obliged to report cybernetic security incidents in their infrastructure. NSA did not accept full abolition of reporting obligation as was proposed. The chosen option ensures full functionality of the system while respecting the minimal approach. Also the proposal to declare the state of cybernetic emergency by the Prime Minister has been accepted. The state of cybernetic emergency shall be declared by the Prime Minister on the basis of proposal by the NSA Director. Provisions dealing with responsibility for damages were added to the draft. The definitions of terms were adjusted and broadened in line with comments by CZ.NIC z.s.p.o. The document was adjusted in regard to the processing of personal data. The personal data will not be required and shall be handled in accordance with the law in case of their transfer.

Another channel for consultations was meeting to present the basic idea of the regulation with the wide spectrum of representatives of expert public, academic sphere and public governance which took place on 22nd November 2011. The journalists were invited as well. The conclusions of the working group drafting the legislative intent of the Law on cybernetic security were presented for the first time by representatives of the NSA and Masaryk University Brno. The conclusions were widely accepted. Vague objections aiming to the fact that the results of the research task of the Ministry of Interior were not used. Another discussed topic was vagueness of proposed counter-measures.

The legislative intent was presented also to the Council for cybernetic security. The Council is advisory body of the Prime Minister for the field of cybernetic security. Its members (designated representatives of Ministry of Interior, Ministry of Defence, Ministry of Foreign Affairs, Ministry of Finance Ministry of Trade and Industry, Ministry of Transport, Police, Office for Foreign Relations and Information, Security Intelligence Service, Military Intelligence, Office for Protection of Personal Data, CTO) discussed the

draft which was adjusted according to their comments and submitted to the inter-ministerial consultation procedure.

Concurrently, it was presented to the public at the webpage of the NSA. The comments of the public sent to the NSA aiming to specify obligations during the state of cybernetic emergency and to clarify structure of bodies active in cybernetic security , were accepted.

The proposal to limit the scope of the legislative intent only to public sector and information systems of public governance was not accepted because such requirement goes against the principle of division of cyberspace to critical part (of both informational and communication infrastructure) and the rest of the cyberspace, regardless of the status of the respective entity.

The document was also presented to the working group of the Legislative Council of the Government for impact assessment evaluation. The representatives of the NSA were invited to the session of the working group and evaluation by the expert public was presented to them by member of the working group Prof. Ing. Petr Moos, CSc. The comments were settled on 14th March 2012 at the meeting at the Transport Faculty of the ČVUT. The document was adjusted in the following way: the method for determination of elements of critical infrastructure will be based on the current system of the Crisis Law; The terminology dividing critical infrastructure to critical communication infrastructure and critical information infrastructure will be abandoned and the united term critical information infrastructure will be used in future; Security standards will be based on standards ISO/IEC 20 000 a ISO/IEC 27 000; The terms describing the teams contributing to the protection of the cyberspace will be changed to be in compliance with usual international terminology. Instead of the National Supervisory Site, term Governmental CERT will be used for the facility supervising critical information infrastructure and information systems of public governance. Similarly, the term National CERT will be used for the facility supervising private providers and network administrators instead of Central Supervisory Site; Also the part dealing with declaration of the state of cybernetic emergency and responsibility for adopted measures. The comment aiming to absence of technical analysis based on research document “Issue of cybernetic threats from the point of view of security interests of the Czech Republic” has been clarified. Due to the fact that the results of this

research were handed over to the NSA only on 20th March 2012, it was not possible to provide such analysis. It should be noted that the results of this research are inadequate and unusable and cannot be used for any analysis of technical situation. The drafted legislative intent is legal background for technical solution based on respecting the maximum of the current technological solution of entities which are subject to regulation and technologically neutral security measures based on international standards.

6.2 Contacts, declaration on approval of impact assessment

National Security Authority – Department of Law and Legislation
Phone number to the secretary of the department: 257 283 439
E-mail to secretary of the department: pravni@nbu.cz
Person responsible for the final report on regulation impact assessment
Mgr. Jiří Malý
Legislative branch of Department of Law and Legislation
Phone: 257 283 325
E-mail: j.maly@nbu.cz.

B: Draft substantial solution

7. Definitions

The intent is based on legislative technique and defines only specific terms or terms whose interpretation in common language may be confusing. The following term will be legally defined:

- Cyberspace – digital environment allowing for creation, processing and exchange of information; composed of information and communication technologies including connection to the public network (internet).
- Czech cyberspace - digital environment allowing for creation, processing and exchange of information; composed of information and communication technologies whose functioning is regulated by the legal system of the Czech Republic, including connection to the public network (internet
- Cybernetic security – complex of legal, administrative, technical, physical and educational activities aimed at ensuring undisturbed and flawless functioning of cyberspace.
- Critical information infrastructure – element of critical information infrastructure or system of such elements whose disruption could cauie damage or harm to the interest of the Czech Republic.
- Interest of the Czech Republic means preservation of its constitutional framework, sovereignty, territorial integrity, internal security, international obligation and defence, protection of economy and life and health of natural persons.
- Element of critical information infrastructure – information system, service[43)] or network of electronic communications[44)] with significant importance for cybernetic security of the Czech Republic whose long-term non-functionality would mean endangering or harm to particular interest of the Czech Republic which is included in the list of elements of critical information infrastructure.

[43)] section 2 letter n) of Law n. 127/2005 Coll., on electronic communications.

[44)] section 2letter h) of Law n. 127/2005 Coll.

- Cybernetic security incident – an event with impact on services or networks of electronic communications or information systems, presenting breach of their security and rules for their protection able to endanger or threaten interest of the Czech Republic listed in the list of cybernetic security incidents issued in the form of NSA regulation.
- Administrator of information system of critical information infrastructure – entity determining the purpose and the means of processing of information and is responsible for the element of critical information infrastructure.
- Administrator of communication system of critical information infrastructure – entity providing service of electronic communication included in critical information infrastructure.
- National Centre for Cybernetic Security –integral part of NSA active in cybernetic security directly subordinated to the NSA Director.
- National CERT/CSIRT – A site operated usually by private entity on the basis of public-law contract ensuring and mediating exchange of information (reporting of security incidents, vulnerabilities etc.) in national and international environment (also as contact pint of last instance), particularly for private entities, academic sphere, self-government provided that none of these entities falls entirely or partially into competence of the NSA. National CERT/CSIRT coordinates its activities with NSA.
- Governmental CERT/CSIRT – working site operated as integral part of the National Centre for Cybernetic Security to protect services and networks of electronic communications and information systems against cybernetic security incidents.
- State of cybernetic emergency – state declared by the Prime Minister of the Czech Republic on the basis of proposal by the NSA Director in case of grave danger to the security of services or networks of electronic communications or information systems causing danger or harm to the interest of the Czech Republic and the danger could not be repulsed by normal means of National Center for Cybernetic Security.

- Counter-measures – operations and activities necessary to protect networks of electronic communications or information systems against negative impact of cybernetic security incident (p.e. installation of new version of antivirus, adjustment of security rules of the firewall, installation of security patch of the information system).
- Security measure – technologically neutral measure not describing particular technology, producer or service provider in order not to determine security solutions used by the regulated entities. The measures shall be issued in the form of NSA regulations and shall be in line with international standards and norms (in particular norms ČSN ISO/IEC 20 000 a ČSN ISO/IEC 27 000, being the basic inspiration during creation generally applicable regulation stating security measures. A holder of ISO/IEC 20 000, resp. ISO/IEC 27 000 will only have to fulfil complementary security measures exceeding framework of security measures included in the aforementioned norms.

8. Scope of effect

8.1 Material authority

The meaning and aim of the law is protection of the Czech cyberspace to provide entities under the jurisdiction of the Czech Republic adequate tools and standards for cybernetic security of their information systems and electronic communication and undisturbed exercise of their right for informational self-determination. The material authority dealing with legal relations to information and communication infrastructure is corresponding to this aim.

The division of material authority is determined by the fact that the cyberspace of the Czech Republic can be divided into critical (with high significance for functioning of the state) and the remaining part (all other services of electronic communications and services of information society). The intent of the law incorporates both networks and services of electronic communications as well as information systems comprising together critical information infrastructure as parts of critical infrastructure of the Czech cyberspace.

Regarding the rest of the communication and information infrastructure, the intent covers only the communication segment – services and networks of electronic communications. It specifically covers information systems of the public governance – systems also covered by law n. 365/2000 Coll., while the legal regulation shall not cover all the administrators of the public governance information systems to the same degree.

Critical information infrastructure for the purposes of the law on cybernetic security shall be defined in accordance with the principles of the law n. 240/2000 Coll. on crisis management (Crisis Law). Elements of critical infrastructure in the field of cybernetic security shall be defined by the way determined by the Crisis Law and Governmental regulation n.. 432/2010 Coll. The elements in the private sphere shall be determined by general regulation issued by the NSA according to the administrative law. The elements in the sphere of public governance shall be determined by the decision of the Government, based on NSA proposal. The elements of critical infrastructure in the field of cybernetic security will be subject to the same general obligations pursuant to the Crisis Law as well as specific obligations stated by the Law on cybernetic security.

8.2 Personal Authority

The new regulation shall have effect on the following groups of entities:

- *Electronic communication service providers and administrators of electronic communication networks*. These entities shall be obliged to report to national CERT/CSIRT contact details for the purposes of exchange of information and selected administrators of electronic communication networks shall have obligation to report cybernetic security incidents occurring in their networks to national CERT/CSIRT. The criteria for selection shall be determined in accordance to the impact the possible non-functionality of such networks as agreed with national CERT/CSIRT. In case of declaration of state of cybernetic emergency, all electronic communication service providers and entities operating networks shall also be obliged to implement counter-measures ordered by the NSA.
- *Administrators of systems of communication infrastructure included in critical information infrastructure.* It is a sub-group of electronic communication service providers and administrators of electronic communication networks. These

entities shall be obliged to report to the NSA contact details for immediate exchange of information and report selected cybernetic security incidents related to the communication infrastructure included in critical information infrastructure to the NSA. They shall be obliged to protect communication systems included in critical information infrastructure (elements of critical information infrastructure) by security measures stated by the NSA in the form of ordinance. Unlike the general electronic communication service providers and administrators of electronic communication networks they will be obliged to implement counter-measures ordered by the NSA also in the normal regime outside of the state of cybernetic emergency. The extent of the measures shall be determined by the decision or provision of general nature.

- *Administrators of information systems included in critical information infrastructure.* These entities shall be obliged to report to the NSA contact details for immediate exchange of information and report selected cybernetic security incidents related to the information systems of critical information infrastructure to the NSA. They shall be obliged to protect information systems included in critical information infrastructure (elements of critical information infrastructure) by security measures stated by the NSA in the form of ordinance. They will be also obliged to implement counter-measures ordered by the NSA. The extent of the measures shall be determined by the decision or provision of general nature.

- *Administrators of information systems of public governance*[45)]*.* They are ministries, other administrative offices and entities of territorial self-governance that determine the purpose and means of processing of information and are responsible for information systems in accordance with law n. 365/2000 Coll. The obligation to protect the information systems of the public governance by security measures shall be stated. Parameters of those measures shall be determined by the NSA in the form of ordinance (lower standard than administrators of information systems included in critical information infrastructure) only for significant systems (such measures cannot be implemented in non-significant systems). The law shall state criteria for

[45)] Section 2 letter c) of law n. 365/2000 Coll., on informatik systems of public governance.

determination of significance of an information system. The selected administrators of information systems of public governance shall be obliged to report selected cybernetic security incidents to the NSA and implement counter-measures ordered by the NSA.

8.3 Territorial authority

The legislative intent does not intend to state specific territorial effect of the law.

8.4 Time authority

The law plan to state in particular obligations to report cybernetic security incidents and measures to protect information and communication systems. It therefore necessary to provide them with sufficient time for implementation of these measures. On the other hand, it can be taken into account that the reporting and protective measures are already implemented by many of the entities being subject to the new regulation and their adaptation should therefore not be too difficult.

Time limits to fulfil the obligations shall be stated in the following way:

- *Electronic communication service providers and administrators of electronic communication networks* – obligation to report contact details for exchange of information: 30 days after the law comes to force; obligation of selected electronic communication service providers and selected administrators of electronic communication networks to implement reporting of selected cybernetic security incidents: 1 year after the law comes to force at the latest; obligation to implement counter-measures ordered by the NSA in the state of cybernetic emergency: 1 year after the law comes to force at the latest.
- *Administrators of systems of communication infrastructure included in critical information infrastructure* - obligation to report contact details for exchange of information:: 30 days after the law comes to force; obligation to implement reporting of selected cybernetic security incidents: 1 year after the law comes to force at the latest; obligation to implement security measures stated by the NSA in the form of ordinance: 1 year after the law comes to force at the latest;

obligation to immediately implement counter-measures ordered by the NSA: 1 year after the law comes to force at the latest.

- *Administrators of information systems included in critical information infrastructure* - obligation to report contact details for exchange of information:: 30 days after the law comes to force; obligation to implement reporting of selected cybernetic security incidents: 1 year after the law comes to force at the latest; obligation to implement security measures stated by the NSA in the form of ordinance: 1 year after the law comes to force at the latest; obligation to immediately implement counter-measures ordered by the NSA: 1 year after the law comes to force at the latest.
- *Administrators of information systems of public governance* - obligation to report contact details for exchange of information: 30 days after the law comes to force; obligation of selected administrators of information systems of public governance to implement reporting of selected cybernetic security incidents: 1 year after the law comes to force at the latest; obligation to immediately implement counter-measures ordered by the NSA: 1 year after the law comes to force at the latest. The contact details shall be transmitted to the public information systems which contains basic information on availability and content of available information systems of public governance (information system on ISs of public governance) operated by the Ministry of Interior in accordance with section 4 para. 1 letter h) of the law n. 365/2000 Coll. The content of this information system shall be supplemented with contact details explicitly for the purposes of the Law on cybernetic security. Obligation of selected administrators of information systems of public governance to implement security measures stated by the NSA in the form of ordinance: 1 year after the law comes to force at the latest.

9. NSA, National Centre for Cybernetic Security and supervisory bodies

According to the decision of the Government of the Czech Republic n 781 dated 19th October 2011, the NSA has been awarded national authority over cybernetic security issues. organisation of centralised evaluation of information concerning cybernetic

security in the Czech Republic will be based on two supervisory bodies - governmental CERT/CSIRT and national CERT/CSIRT. Governmental CERT/CSIRT will be part of the national Centre for Cybernetic Security. National CERT/CSIRT will be operated by private entity on the basis of public-law contract with the NSA.

The law shall regulate:

- *NSA as state body responsible for state governance in the field of cybernetic security.* The NSA shall evaluate data about cybernetic security incidents acquired from the supervisory bodies, issue implementing regulations, check and sanction noncompliance with obligations stated by the law on cybernetic security, propose declaration of state of cybernetic emergency, act as coordination body in the case of cybernetic emergency and cooperate with other state bodies.
- *National Centre for Cybernetic Security as NSA department working in the field of cybernetic security and directly subordinated to the NSA Director.* National Center for Cybernetic Security will be integral part of the NSA. It will contain governmental CERT/CSIRT and administrative divisions providing support for its functioning. It will cooperate with other supervisory bodies (CERTs/CSIRTs), ensure international cooperation, cooperation with research and development facilities, prepare implementing regulations, technical parameters (standards) and recommendations (best practices), prevention and education in the field of cybernetic security. National Centre for Cybernetic Security will work in research and development of mean and analyse vulnerabilities. National Centre for Cybernetic Security will check fulfilment of administrators of information and communication systems included in critical information infrastructure and administrators of selected information systems of public governance and shall hand over its findings to other NSA departments (p.e. for administrative sanctioning). The current competences of the Ministry of Interior over administrators of information systems of public governance according to law n. 127/2005 Coll. shall remain untouched.
- Governmental CERT/CSIRT shall evaluate data from critical information infrastructure and information systems of public governance. In case of cybernetic security incident it will cooperate with administrator of the respective

system or network. The NSA will order counter-measures in case of no response from the administrator.

- National CERT/CSIRT – facility operated by private entity on the basis of public-law contract ensuring and facilitating exchange of information (reporting of security incidents and vulnerabilities) in national and international context (also as contact point of last instance) first of all for private entities, academic sphere, self-government, non-profit sector in case these entities are not subject of regulation by the NSA. National CERT/CSIRT coordinates its activities with NSA.

National Centre for Cybernetic Security shall evaluate information on cybernetic security incidents from:

- administrators of systems of communication infrastructure included in critical information infrastructure,
- administrators of information systems included in critical information infrastructure,
- administrators of information systems of public governance,
- supervisory bodies.

It will also provide the abovementioned entities with information about cybernetic security situation, on evaluated cybernetic security incidents or methodology and assistance during their solution. National Centre for Cybernetic Security shall cooperate with respective bodies of partner states (states with which the cooperation in the field of cybernetic security on ministerial or higher level has been established), similar facilities of international organisations, non-governmental organisations and issue parameters of security measures and non-binding recommendations (best practices) for public and private sector in the form of announcements in the Bulletin of NSA.

The NSA shall directly lay down concrete counter-measures to solve cybernetic security incidents in the form of decisions or general purpose provisions to:

- administrators of systems of communication infrastructure included in critical information infrastructure,
- administrators of information systems included in critical information infrastructure,

- administrators of information systems of public governance,
- also other electronic communication service providers and entities operating networks of electronic communications during the state of cybernetic emergency.

CTO shall be informed about counter-measures ordered to administrators of systems of communication infrastructure included in critical information infrastructure which shall have impact on the public.

10. Public bodies

The law shall impose obligation on those public governance bodies which administer information systems of critical information infrastructure (those corresponding to definition of administrator of information system of critical information infrastructure or administrator of communication system included in critical information infrastructure according to the law on cybernetic security) and in a varying extent to those who administer information systems of public governance. These entities will be obliged to report to the NSA contact details for the immediate exchange of information and protect their information systems by security measures whose features will be stated by the NSA in the form of ordinance. They will be also obliged to report the selected cybernetic security incidents to the NSA and implement counter-measures ordered by the NSA.

The respective time limits shall be stated for fulfilment of obligations to report the selected cybernetic security incidents and to implement counter-measures ordered by the NSA (viz time authority).

11. Private entities

It is necessary to impose obligations also to private entities in order to ensure protection of the Czech cyberspace. The law is outlined as minimalist in this regard. It does not intervene into the content of communication and other content-related components of information and communication infrastructure. The law also does not regulate direct execution of state powers. The state only monitors information about security situation in the Czech cyberspace via the national Centre for Cybernetic Security and acts directly only towards systems with critical importance for cybernetic security

of the Czech Republic (elements of critical information infrastructure) and towards the systems of public governance.

In the common regime, the private electronic communication service providers and administrators of electronic communication networks shall only be obliged to report contact details to report to the national CERT/CSIRT, under the threat of sanctions. The selected electronic communication service providers and administrators of electronic communication networks will be obliged to report selected cybernetic security incidents to the national CERT/CSIRT (details on technical specification of cybernetic security incidents and format of reports shall be stated by implementing regulation of the NSA). The national CERT/CSIRT shall besides permanent evaluation of cybernetic security situation also provide methodical assistance and help to the private entities using the reported contact details. The private electronic communication service providers and administrators of electronic communication networks will only be obliged to implement counter-measures of the NSA when the state of cybernetic emergency is declared.

The law shall not distinguish between private and public entities in relation to the critical infrastructure. Due to the critical importance of these systems, the law presumes not only the obligation to report cybernetic security incidents but also to implement security measures and counter-measures ordered by the NSA, regardless the nature of the responsible entity.

Structure of obligations imposed to the private entities shall be the following:

- Electronic communication service providers and administrators of electronic communication networks. These entities shall be obliged to report to national CERT/CSIRT contact details for the purposes of exchange of information and selected administrators of electronic communication networks shall have obligation to report cybernetic security incidents occurring in their networks to national CERT/CSIRT. The criteria for selection shall be determined in accordance to the impact the possible non-functionality of such networks as agreed with national CERT/CSIRT. In case of declaration of state of cybernetic emergency, all electronic communication service providers and entities operating networks shall also be obliged to implement counter-measures ordered by the NSA. The obligations to report to national CERT/CSIRT contact details for the purposes of exchange of information and obligation of selected administrators of

electronic communication networks to report cybernetic security incidents occurring in their networks will be incorporated to the law n. 127/2005 Coll. in the form of reference as obligations to ensure security and integrity of networks and further regulated by the Law on cybernetic security and ordinances of the NSA. These obligations shall be sanctioned by CTO in the framework of its competence. The obligation to implement counter-measures ordered by the NSA during the state of cybernetic emergency shall be based on Law on cybernetic security and non-compliance shall be sanctioned by the NSA.

- *Administrators of systems of communication infrastructure included in critical information infrastructure.* These entities shall be obliged to report to the NSA contact details for immediate exchange of information and report selected cybernetic security incidents related to the communication infrastructure included in critical information infrastructure to the NSA and to t implement counter-measures ordered by the NSA. The obligations to report to the NSA contact details for the purposes of exchange of information and obligation of selected administrators of electronic communication networks to report cybernetic security incidents occurring in their networks will be incorporated to the law n. 127/2005 Coll. and further regulated by the Law on cybernetic security and ordinances of the NSA. These obligations shall be sanctioned by CTO in the framework of its competence. They shall be also obliged to protect communication systems included in critical information infrastructure (elements of critical information infrastructure) by security measures stated by the NSA in the form of ordinance. This obligation and obligation to implement counter-measures ordered by the NSA will be based on Law on cybernetic security and shall be supervised and sanctioned by the NSA.
- *Administrators of information systems of critical information infrastructure (private entities administering information systems included in critical information infrastructure).* These entities shall be obliged to report to the NSA contact details for immediate exchange of information and report selected cybernetic security incidents related to the information systems of critical information infrastructure to the NSA. They shall be obliged to protect information systems included in critical information infrastructure (elements of critical information

infrastructure) by security measures stated by the NSA in the form of ordinance. They will be also obliged to implement counter-measures ordered by the NSA. The extent of the measures shall be determined by the decision or provision of general nature. These obligations shall be regulated by the Law on cybernetic security and supervised and sanctioned by the NSA.

The abovementioned obligations may require implementation of security measures allowing identifying and reporting cybernetic security incidents by the private electronic communication service providers and administrators of electronic communication networks. The investments should not be significant because the respective entities have already implemented such technologies. The NSA and national CERT/CSIRT shall share contact details of private entities for the purpose of imposing counter-measures in case of declaration of state of cybernetic emergency.

The NSA shall lay down the minimal security measures to be implemented by the subjects by the implementing regulation. However, damage may occur even when this obligation is fulfilled. The responsibility for the damage will be solved the standard way – the entity shall be responsible for damage in case of non-compliance with the security measures according to the Civil Code. In case of damage event when the security measures have been properly implemented, the entity shall not be held responsible in case it can prove it put in all efforts that could be demanded from it to prevent the damage. Responsibility of state bodies for damage is also governed by general regulation (see chapter 16).

12. Processing of personal data, operational data and access to information

The proposed regulation does not directly affect processing of personal data[46], operational data[47], localization data[48] or access to information of the public sector. All data being processed by the NSA and national CERT/CSIRT on the basis of the proposed regulation shall deal with cybernetic security incidents and measures for their solution

[46] Section 4 letter a) of law n. 101/2000 Coll., on protection of personal data.

[47] Section 90 para. 1 of law n. 127/2005 Coll.

[48] Section 91 para. 1 of law n. 127/2005 Coll.

and are not related to particular users of electronic communications services or to the content of their communication. The NSA and the national CERT/CSIRT shall not process any information infringing with the right for informational self-determination or that are protected by special laws. However, the special laws shall be respected should the information protected by them occur during processing of cybernetic security incident reports.

The NSA shall store identification data on systems affected by cybernetic security incidents and the method and success of their solution in the database of cybernetic security incidents. Such data may harm interests of the Czech Republic or related entities in case of misuse. Therefore, they shall be protected institute of discreetness. The most significant information with grave importance for the cybernetic security of the Czech Republic shall be protected as classified information in case they fulfil the attributes of classified information in accordance with the Law on protection of classified information (see chapter Records).

13. Records

Processing data on cybernetic security incidents is necessary precondition for their evaluation, development of defence procedures as well as for effective cooperation with the private sphere and international organisations. Data on cybernetic security incidents can also serve for development of better protection technologies. Therefore the legislative intent envisages that the NSA shall have database of cybernetic security incidents.

The reports of cybernetic security incidents as well as implemented counter-measures are information of big security and economic impact. They can lead to identification of the affected system; disclose security methods, counter-measures and vulnerabilities of communication and information infrastructure to the attackers and the like. It is therefore necessary to protect such data against misuse and rule out possibility of their leak. At the same time it is necessary to maintain the advantages of information sharing with other bodies contributing to protection of Czech cyberspace (including national CERT/CSIRT, local CERTs/CSIRTs etc.) as well as provide for standard democratic control of the NSA through the free access to information.

Data identifying the affected system, data identifying the originator of the cybernetic security incident and record on its solution shall be protected by discreetness obligation. Records on solution of grave cybernetic security incidents may have the nature of classified information[49)]. Information from the database of cybernetic security incidents shall be provided to law enforcement bodies and other public bodies if necessary to carry out duties which fall into their competence.

14. Cooperation and following the technical development

Cooperation with private sector, other public governance bodies and foreign entities is necessary precondition for effectiveness of the protection of Czech cyberspace. Exchange of information is basis of such cooperation during building of the system of cybernetic security as well as during solution of particular cybernetic security incidents. Effective solution of large scale cybernetic attacks may be reached by mutual cooperation of supervisory bodies with assistance of local supervisory facilities of state bodies, telecommunication service providers and international organisations.

Bearing in mind rapid technological development, the legislative intent anticipates that technological means of protection defined by the NSA in the form of ordinances shall contain general recommendations in general form – they shall not refer to particular products or producers but to methods and procedures. The law on cybernetic security shall state general conditions for issuing of ordinances regulating security measures and technologies, their possible periodicity and sanctions imposed in case of non-compliance. They shall not contain sensitive information due to the fact that the such technologically important information that could help attackers to create a whole agent system.

14.1 Cooperation with private entities

The NSA shall be eligible to conclude public law contract with the operator of the National CERT/CSIRT. The entity with relevant technical competence shall on the basis of the agreement gather and evaluate data from communication infrastructure and

[49)] Section 2 of law n. 412/2005 Coll., on protection of classified informatik and security eligibility

provide assistance during solving cybernetic security incidents to the private electronic communication service providers and administrators of electronic communication networks. There will be explicit authorisation concerning these activities and the NSA will have to publish the concluded public-law contract in its bulletin.

The NSA shall also cooperate with other private entities, namely local supervisory facilities and research and development bodies.

14.2 Cooperation with public governance bodies and public law corporations

The NSA shall be eligible by the law to cooperate with NBÚ public governance bodies and public law corporations are or will be active in the field of cybernetic security. Besides security structures of the Czech Republic and crisis management bodies they will be mostly particular administrators of information systems, public administrators of critical infrastructure, research and development state-funded organisation, universities etc. The main aim of the cooperation shall be exchange of information, mutual assistance in development and testing of security measures and participation at the exercises. The cooperation does not involve any change to the competences of security structures limiting their current authority or infringe into their rights.

14.3 International cooperation

International cooperation established by the NSA shall include participation in international structures dealing with cybernetic security (in the form of joining international organisations and associations aiming at exchange of information on cybernetic security incidents and coordination of protection activities) and participation at international events. The NSA shall be eligible to conclude international agreement son ministerial level in the field of cybernetic security and to represent the Czech Republic in international organisations and at international events - exercises and simulations.

15. Supervision and sanctions

The effective protection of cybernetic security demands existence and implementation of respective apparatus of supervision and sanctions. Its structure is

derived from the division of cyberspace to critical part and the rest with consideration to specific status of administrators of information systems of public governance. It is also necessary to take into consideration that electronic communication service providers and administrators of electronic communication networks are subject to supervisory and sanction authority of the CTO.

The NSA shall according to the Law on cybernetic security impose obligation to implement security measures to the entities of critical information infrastructure being elements of critical of critical infrastructure and shall sanction their non-compliance. Such measures will supplement obligations imposed on providers in section 98 of law n. 127/2005 Coll. The model of close cooperation with the CTO during preparation of security measures will be applied to minimise impact of such measures. The supervision shall be performed jointly.

Bearing in mind that the legislative intent is drafted as minimalistic as regards to the competences of bodies of public governance, substantial change in competences with regard to electronic communications is not expected. The division of supervisory and sanction powers are based on presumption that the CTO supervises and imposes sanctions in the field of communication infrastructure and specific obligations in the field of cybernetic security are supervised and respective sanctions imposed by the NSA and partially Ministry of Interior.

The intent anticipates the following division of powers:

NSA:

- Power to supervise and impose sanctions to administrators of information systems included in critical information infrastructure. The obligations to report contact details for exchange of information and to report selected cybernetic security incident are subject of supervision and sanctions.
- Power to supervise and impose sanctions to administrators of information systems included in critical information infrastructure (implementation and operation of prescribed security measures in elements of critical infrastructure) including remedy measures and sanctions (at higher level in case of state of cybernetic emergency).

- Power to impose remedy measures and sanctions in case of non-implementation of counter-measure prescribed to the administrator of the information system included in critical information infrastructure (at higher level in case of state of cybernetic emergency).
- Power to supervise administrators of systems of communication infrastructure included in critical information infrastructure (implementation and operation of prescribed security measures in elements of critical infrastructure) including remedy measures and sanctions (at higher level in case of state of cybernetic emergency).
- Power to impose remedy measures and sanctions in case of non-implementation of counter measure prescribed to the administrator of the system of communication infrastructure included in critical information infrastructure (at higher level in case of state of cybernetic emergency).
- Power to impose remedy measures and sanctions in case of non-implementation of counter-measure prescribed to the electronic communication service provider and administrator of electronic communication network in the state of cybernetic emergency.
- Power to supervise and impose sanctions to administrators of information systems of public governance. The obligations to report contact details for exchange of information and to implement counter-measures prescribed by the NSA are subject of supervision and sanctions. Power to supervise and impose sanctions for (non-)reporting of selected cybernetic security incidents to selected administrators of information systems of public governance

CTO (by amendment to law n. 127/2005 Coll.):

- Power to supervise and impose sanctions to administrators of systems of communication infrastructure included in critical information infrastructure (reporting of contact details for information exchange and reporting of cybernetic security incident related to critical information infrastructure).
- Power to supervise and impose sanctions to electronic communication service providers and administrators of electronic communication networks (reporting

of contact details for information exchange and with selected electronic communication service providers and selected administrators of electronic communication networks also reporting of selected cybernetic security incidents in the form prescribed in the NSA ordinance).

Ministry of Interior (by amendment to law n. 365/2000 Coll.):

- Power to supervise selected administrators of information systems of public governance not included in critical infrastructure including imposing remedy measures and sanctions (implementation and operation of prescribed security measures)

The execution of supervisory powers will be based on general provisions of the Law on state supervision[50)] with regard to the drafted regulation. The information that some entities are non-compliant with the obligations prescribed by the Law on cybernetic security and the law n. 127/2005 Coll. will be mostly missing reports on cybernetic security incidents evaluated by the National Centre for Cybernetic Security. Due to this fact the Law on cybernetic security shall give NSA the right to propose to CTO to perform oversight in the respective entity.

16. State of cybernetic emergency

The legislative intent anticipates special regime of the state of cybernetic emergency in case of large-scale cybernetic attack or other serious cybernetic security incident in the territory of the Czech Republic or in international scale. The law on cybernetic security shall prescribe the declaration of the state of cybernetic emergency and associated rights and obligations. The state of cybernetic emergency shall be regulated outside the framework of Crisis Law similarly as the state of emergency according to the law n. 458/2000 Coll., on conditions of entrepreneurship and performance of state administration in the filed of energetic (Energetic Law).

[50)] law n. 552/1991 Coll., on state oversight.

The state of cybernetic emergency shall be declared by the Prime Minister of the Czech Republic on proposal of the NSA Director. His decision has to be approved by the Government in 24 hours (if not, the decision on declaration of the state of cybernetic emergency is cancelled by expiration of this time limit). The state of cybernetic emergency may be declared for no more than seven days. Prolongation for another seven day period may be done by the Government (even repeatedly).

The NSA Director shall call together the Commission for Cybernetic Security after the declaration of the state of cybernetic emergency. The Commission shall be advisory body of the NSA Director, proposing measures for protection of Czech cyberspace and ensuring communication with the respective national and foreign entities. The Commission will be chaired by the NSA Director and further composed of representatives of public governance, intelligence services and private entities active in the field of critical information infrastructure. The Commission shall continuously evaluate its actions and inform the Government via the NSA Director. In case of intensity of cybernetic security incidents endangering to great extent lives, health, property, internal order or security of the Czech Republic, the NSA Director shall inform the Government that declaration of state of emergency is necessary[51)].

The only significant change for private entities in the state of cybernetic emergency according to the Law on cybernetic security will be the obligation to electronic communication service providers and administrators of electronic communication networks to implement counter-measures prescribed by the NSA. Counter-measures shall be announced through the contact details reported by the providers to the National CERT/CSIRT and shared with the NSA.

The regulation of the state of cybernetic emergency shall be placed in the Law on cybernetic security since it is special regime according to this law and does not infringe into rights and obligations of entities outside its personal authority.

In case of damage occurred during the state of cybernetic emergency, the state shall be responsible only if the conditions of the law n. 82/1998 Coll., *on responsibility for damages caused during performance of public governance by decision or incorrect official procedure* are fulfilled.

[51)] Čl. 5 ústavního zákona č. 110/1998 Sb.

17. Implementing regulations and recommendations

The intent anticipates the use of implementing regulations to specify technical details of obligations of electronic communication service providers, administrators of electronic communication networks, administrators of systems of communication infrastructure included in critical information infrastructure, administrators of information systems included in critical information infrastructure and administrators of other information systems of public governance. Besides the implementing regulations the intent also anticipates use of parameters of security measures and non-obligatory recommendations issued in the NSA bulletin.

The NSA shall issue in the form of ordinances:

- Technical details for identification of cybernetic security incidents and typology of incidents (with regard to possible damage and to information level of the cybernetic security incident) and technical details for reporting of the cybernetic security incidents.
- Technical details of security of information systems of critical information infrastructure.

18. Amendments to other legal regulations

The legislative intent anticipates the amendment to section 98 of law n. 127/2005 Coll., specifying obligations to ensure security and integrity of electronic communication in the form of reference to specific obligations of electronic communication service providers and administrators of electronic communication networks described in the new Law on cybernetic security and NSA ordinance.

Law n. 365/2000 Coll. shall be amended:

- Authorisation to issue ordinance on security of information systems of public governance (with the exception of those included in critical infrastructure) will be proposed.

- Provisions on information system of information systems of public governance shall be amended to provide for exchange of contact details for the purposes of law on cybernetic security. A mark that information system is included in critical information infrastructure shall be part of the entry in the information system.

Crisis law shall be amended.

- A new provision dealing with NSA powers in the field of cybernetic security may be added to the law. It will describe the differences from the general regulation if required by the law on cybernetic security. Minimal level of security measures to be implemented by the elements of critical infrastructure in the field of cybernetic security shall be prescribed in the new Law on cybernetic security or the respective implementing regulation of the NSA who will serve as guarantor of such provisions.

Regulation of the Government n. 432/2010 Coll., on criteria for determining the element of critical infrastructure shall be amended.

- General criteria shall be amended (in particular point of view of time may be considered). The amended general criteria shall be applicable to determination of all elements of critical infrastructure including the field of cybernetic security, to newly incorporate needs for protection of cyberspace and possible impacts of cybernetic security incidents. The sector criteria shall be also amended to adapt to the fact that the field of cybernetic security will be a new part of sector "VI. COMMUNICATION AND INFORMATION SYSTEMS". Administrator of the new sub-sector shall be NSA with respect to its new authority given by the Law on cybernetic security. The NSA shall be responsible for proposing and determining the elements of critical infrastructure in the sub-sector COMMUNICATION AND INFORMATION SYSTEMS - cybernetic security.

It cannot be excluded that the need to amend another laws and regulation will arise during preparation of the draft law. The extent of such amendment will not be significant.

19. Constitutional conformity

With respect to current judicature of the Constitutional Court[52)] there is need to evaluate this intent by the standard test of proportionality. The basic right that will be limited by the Law on cybernetic security will be the right to property and partially also derived right to entrepreneurship. The intent does not infringe to the following rights due to the fact that the minimalist approach towards private entities has been chosen: the right for protection of privacy, right for protection of personal data, right for private life, freedom of speech and other rights designated as rights for informational self-determination.

Cybernetic security incidents not only cause damages but also limit availability of services of information society or violate one's information privacy. The right for informational self-determination was first identified by German Federal Constitutional Court[53)] followed also by the European Court for Human Rights and the Constitutional Court of the Czech Republic[54)]. It consists from passive and active information rights of a person. Passive information rights include protection of privacy and generally discrete information sphere while the active rights involve access to services of information society. It means that the definition of informational self-determination is based not only on protection of discrete data but also on the presumption that person can live full life only with access to communication with others. The state is obliged to protect both passive and active rights by the protection of cyberspace.

The Law on cybernetic security will limit only private owners and operators of communication infrastructure - electronic communication service providers and administrators of electronic communication networks. The limitation of right to property and entrepreneurship bears the form of the obligation to report contact details to the National CERT/CSIRT and for selected electronic communication service providers and selected administrators of electronic communication networks to report

52) Finding of the Constitutional Court dated 12th October 1994, file mark Pl.ÚS 4/94, 214/1994 Coll., N 46/2 SbNU 57.

53) Finding of the Federal Constitutional Court dated 15th December 1983, n. BVerfGE 65, 1.

54) Finding of the Constitutional Couret dated 1st March 2000, n. II. ÚS 517/99, N 32/17 SbNU 229, Finding of the Constitutional Court dated 7th April 2010, n. I. ÚS 22/10 and fading of the Constitutional Court dated 22nd march 2011, file mark Pl. ÚS 24/10, 94/2011 Coll.

selected cybernetic security incidents. That is an infringement into the *iuris utendi* to the respective communication infrastructure.

Specific obligations are imposed on entities operating systems included in the critical information infrastructure. Besides the obligation to report cybernetic security incidents to the NSA, they also have to implement security measures in line with the prescribed standard and to react to NSA requirements to adopt counter-measures.

The proposed regulation does not directly infringe into the right to informational self-determination because it does not deal with content of the communication and does not provide for direct powers of the state to intervene into common life of the information society – the law does not presume any intervention into the privacy of the users or to their ability to communicate.

The right for the informational self-determination is a value to protection of which is the new law primarily aimed. Security is not a value "per se". It has to be clear what has to be secured. In this case the law uses clear teleology of protection of the Czech cyberspace – ensuring the functioning of services of information society, both public and private. Free execution of right for informational self-determination could only be achieved through these services, their availability, reliability and security[55)].

The basic principle of the international law of *due diligence* is beside the obligations stemming from membership in international organisations the main reason for the regulation of cybernetic security. It is only matter of time when the International Court Tribunal will start to solve the responsibility of the state for actions not taken by it but attributable to it because they occur it its sovereign domain. The typical situation may be that a computers in the Czech Republic are used for attack at foreign state (a common case with large-scale attacks). The Czech Republic although it is not involved and is not organising such attack may be called to responsibility because it did not prevent the attack while it had capabilities to do so.

The abovementioned infringement into the law to property of private electronic communication service providers and administrators of information and communication systems included in critical infrastructure is in the terms of proportionality justified by the protection of:

[55)] Zpráva Zvláštního zpravodaje Valného shromáždění OSN č. A/HRC/17/2.

- right for informational self-determination (in particular protection of privacy, private life, freedom of speech, access to information and other human rights),
- security and integrity of the Czech Republic and
- international obligations of the Czech Republic.

Following are brief conclusions regarding the constitutional conformity of the legislative intent:

- *Test of suitability* – the intent will undoubtedly lead to the enhancement of the cybernetic security of the Czech Republic and protection of the abovementioned values. The experience shows that the exchange of information about cybernetic security incidents and coordination of efforts are the most effective tools for the protection of cyberspace. The intent is based on current ICT knowledge and chooses the most effective tools for cyberspace protection while maintaining minimal burden on private entities.
- *Test of necessity* – the conducted studies did not find an alternative solution that could fulfil the main goal of the intent – the protection of the cyberspace of the Czech Republic. Although the majority of electronic communication service providers is well motivated to contribute to the cybernetic security of the state by economy (only functioning network can generate income), it is necessary to ensure also the contribution of entities which neglect (because of ignorance, incompetence or intentionally) the protection of their own infrastructure by legal means. Such entities endanger the whole of the Czech cyberspace and emphasis has to be given to those, whose infrastructure is critically important for the state.
- *Test of appropriateness* – The infringement into the law for property is in obvious disproportion to the distributive and non-distributive rights for whose protection it is established. The obligation to report cybernetic security incidents, implement security measures and guidance does not reach the intensity of the associated risks of economic losses, shocks of the society and loss of international credibility of the Czech Republic. As far as intensity is concerned, the infringement to the right for property and free entrepreneurship are more significant p.e. in the sphere of fire-fighting. The proposed regulation does not infringe into information rights - the particular components to the right for

informational self-determination. The obligations intended by the law are fully justified by the significance of protected interests and limit their subjects only to the necessary level. It may be stated that the proposed regulation is proportional.

It can be stated that since the intent brings only minimal new obligations, does not burden the right for informational self-determination (does not give state bodies powers to infringe into privacy or active communication of users of information services) and significantly raises the protection of fundamental rights and non-distributive public property, it is in line with the requirement of constitutional proportionality and is in conformity with the Constitution.

20. Evaluation of conformity of the proposed regulation with the international agreements binding for the Czech Republic and with acquis communitaire

The cybernetic security is not the subject of international or European law in its complexity. There are many documents regulating the issues of cybernetic security, electronic communication services, critical infrastructure and protection of privacy in electronic communications. The legislative intent is fully in line with current international agreements dealing with the issues mentioned above.

It is first of all the Charter of Fundamental Rights of the European Union, further the Directive 98/34/EC of the European Parliament and of the Council of 22 June 199, 8 laying down a procedure for the provision of information in the field of technical standards and regulations, as amended by Directive 98/48/ES, Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity, the Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive), as amended by Directive 2009/140/ES, Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of

electronic communications networks and services (Authorisation Directive), as amended by Directive 2009/140/ES, Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), As amended by Directive 2009/140/ES, Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive), as amended by Directive 2009/136/ES, Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks, Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection

Further relevant parts of acquis communitaire: Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency and Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice. Further 92/242/EEC: Council Decision of 31 March 1992 in the field of security of information systems, 2002/465/JHA on joint investigation teams, 2002/C 43/02 on a common approach and specific actions in the area of network and information security, 2003/C48/01 on a European approach towards a culture of network and information security, 2005/222/SVV on Attacks against Information Systems, 2009/C62/05 on Common working strategy in the field of fight against computer crime, 2009/C321/01 on a collaborative European approach to Network and Information Security.

The issue is also regulated by the documents of the Council of Europe: Convention of the Council of Europe n. 185 Convention on Cybercrime, Convention of the Council of Europe n. 196 Council of Europe Convention on the Prevention of Terrorism,

Recommendation of the Parliament Assembly n. 1706 (2005) Media and terrorism, Recommendation of the Parliament Assembly n.1565 (2007) How to prevent cybercrime against state institutions in member and observer states?, Recommendation of the Committee of Ministers CM/Rec(2011)8E dated 21st September 2011 on the protection and promotion of the universality, integrity and openness of the Internet, Recommendation of the Committee of Ministers CM/Rec(2008)6E dated 26th March 2008 on measures to promote the respect for freedom of expression and information with regard to Internet filters, Recommendation of the Committee of Ministers Rec(2001)8E dated 5th September 2011 on self-regulation concerning cyber content (self-regulation and user protection against illegal or harmful content on new communications and information services), Recommendation of the Committee of Ministers Rec(95)13E dated 11th September 1995 Concerning problems of criminal procedural law connected with information technology, Declaration by the Committee of Ministers Decl-21.09.2011_2E dated 21st September 2011 on Internet governance principles, Declaration by the Committee of Ministers Decl-28.05.2003E dated 28th May 2003 on freedom of communication on the Internet, Recommendation of the General Assembly 1670 (2004) Internet and Law, Declaration by the Committee of Ministers Decl-07.12.2011_2E dated 7th December 2011 on the protection of freedom of expression and freedom of assembly and association with regard to privately operated Internet platforms and online service providers.

Other documents dealing with cybernetic security and associated issues are Action Plan of the European Union for fight against Terrorism (INI/2004/2214); European Parliament, Security of Information Systems and Networks: Towards the culture of security; OSCE, Report of the Special Rapporteur on support and protection of the freedom of speech n. A/HRC/17/27; OSN, Decision of the Council of Ministers of OSCE n. 3/2004 On fight against use of internet for the purposes of terrorism dated 7th December 2004 and Action plan of G8 countries for fighting high-tech crime.

The legislative intent of the law on cybernetic security is fully in line with international agreement binding for the Czech Republic and is fully compatible with acquis communitaire.

21. Anticipated economic and financial impact of the proposed regulation, impact on state budget, other public budgets, entrepreneurial environment of the Czech Republic, social impacts and impacts on environment.

The proposed legislative intent will have impact on state budget in association with establishment of the national Centre for Cybernetic Security. It will require increase of positions and the budget of the NSA. The Government of the Czech Republic in its Decision n. 781 dated 19th October 2011 approved: transfer of one position and the respective salary and other costs and transfer of 500 thousand CZK from the Ministry of Interior to the NSA in 2011, increase of 8 positions in 2013, 10 positions in 2014 and 5 positions in 2015 NBÚ as well as increase of the NSA budget to operate the National Centre for Cybernetic Security of 51.5 mil. CZK in 2012, of 61 mil. CZK in 2013, of 61 mil. CZK in 2014 and of 65 mil. CZK in 2015.

It is expected that the draft legislative intent will have further insignificant impacts on state and other public budgets and entrepreneurial environment, especially in regard to the new obligations of electronic communication service providers and administrators of electronic communication networks, administrators of systems of communication infrastructure included in critical information infrastructure, administrators of information systems included in critical information infrastructure and administrators of information systems of public governance. The draft is based on assumption that the respective entities already implement security measures and the cost will be mainly in improving their compatibility with technologies used by the supervisory bodies.

The draft legislative intent of the Law on cybernetic security brings neither negative social impacts nor impacts on environment and has no impact on equality of men and women.