Petr Hruza*

RESILIENCE AND PROTECTION OF CRITICAL INFORMATION INFRASTRUCTURE

The article deals with resilience and protection of critical information infrastructure elements. The elements affect rapid recovery of the system to its original state and the increase of resistance during the subsequent emergency events. The article also deals with sectoral and cross-sectional criteria for determining the critical information infrastructure elements, which are closely related to resilience and protection. Risk assessment has been conducted in the area of critical information infrastructure. Finally, amendments of the Czech Cyber Security Act have been mentioned.

Keywords: *cybersecurity, resilience, protection, critical information infrastructure*

1. Critical infrastructure and criteria

According to the Act No 240/2000 Coll. on Crisis Management and on Amendments of Certain Acts (Crisis Management Act), **critical infrastructure (CI)** shall denote the **element of critical infrastructure or the system of elements of critical infrastructure, disruption of which would have a significant impact on the state security, on ensuring the basic living needs of the population, on health of people and state economy**. The CI elements are operated by state institutions or private entities. **The European critical infrastructure** shall denote the critical infrastructure within the territory of the Czech Republic, disruption of which would have a significant impact also on another member state of the European Union. **Element of critical infrastructure** shall denote primarily a building, an establishment, a vehicle or public infrastructure, determined in accordance with the cross-cutting and sectoral criteria. The Ministry of Interior (the General Headquarters of Fire Rescue System of the Czech Republic) administers the list of elements of CI. At present there are about 1300 of such elements [1].

In order for an element is to be determined as a part of critical infrastructure it has to meet **cross-cutting and sectoral criteria** having been set by the government regulation No 432/2010 Coll. on the criteria for determining the element of critical infrastructure [2].

The Cross-cutting criteria are considered to be the set of general criteria for assessing seriousness of impact of disruption or destruction of critical infrastructure element with the limit values which include the following [2]:

a) number of casualties (the injured and the dead);
b) economic impact (economic losses or deterioration of the quality of goods or services, including possible impacts on the environment);
c) impact on public (impact on public confidence, physical deprivation and disruption of everyday life, including the loss of necessary services).

The cross-cutting criteria include the aspects of casualties exceeding 250 dead or 2500 people treated in hospital for the period longer than 24 hours, economic impact with the limit value of state economic loss being higher than 0.5 % of GDP, or impact on public as a result of extensive restriction of provision of essential services or other serious intervention into everyday life affecting more than 125 000 people [2].

The Sectoral criteria shall denote technical or operational criteria determining critical infrastructure elements in particular CI sectors, such as e.g. energy, water management, food industry and agriculture, transport and public administration. Public administration then includes e.g. welfare system, state social support or social assistance [2].

The critical infrastructure is very extensive and it is assumed that the state will continuously protect it. The problem is that not all the CI entities belong to the state assets. Some CI entities are owned by the private sector. Even bigger disproportion can be seen in the area of **critical information infrastructure** (CII), in which the entities are owned mainly by the non-state (private)

* **Petr Hruza**
Department of Tactics, Faculty of Military Leadership, University of Defence in Brno, Czech Republic
Email: petr.hruza@unob.cz

 https://doi.org/10.26552/com.C.2018.2.110-114

sector. Therefore, the protection of the CI becomes a complicated process for the state [2].

2. Critical information infrastructure

Large computer networks, information systems and information services play absolutely essential role in a society. Their reliability and security is necessary for economic and social activities of individual states, and, mainly, for the functioning of state internal market.

The increasing range, frequency and impact of security incidents represent significant threats for the functioning of computer networks and information systems. Computer networks and mainly information systems may also become easy targets for intentional, detrimental actions aimed at damaging or disrupting the operation of systems. Such incidents may cause significant financial losses, breach users´ confidence and cause considerable damage to the state economy as a whole. Management of critical information infrastructure is complicated and mutually interconnected through all the sectors and with high number of participating entities and Czech public administration authorities. It requires a whole number of technical, organizational and other supporting elements with enough time necessary for its solution.

The **Critical information infrastructure** may be perceived as a complex of information and communication systems (meeting the determined cross-cutting and sectoral criteria in the area of cyber security), non-functioning of which may cause a significant impact on the state security, people´s basic necessities of life, health, and on state economy. Critical information infrastructure shall denote the element or the system of the CI elements (according to § 2, letter g) and letter i) of the Act No. 240/2000 Coll.) in the sector of communication and information systems, the area of cyber security (§ 2 letter b) of the Act No. 181/2014 Coll.). In practice they are such information or communication systems (e.g. ICS/SCADA systems), which meet criteria for determining the elements of critical information infrastructure [3].

There have not been signed any international agreements in the area of cyber security yet. The Council of Europe Convention on Cybercrime, known also as Budapest Convention, deals with cybercrime to a minor extent. The Act on Cybersecurity and its implementing regulations are rather non-binding recommendations and obligations to protect important information systems formulated e.g. in the reports of the UN Group of Governmental Experts (UN GGE) or in the confidence building measures taken by the OSCE member states. The judicature of the European Court of Human Rights does not deal directly with cyber security either [3].

The critical information infrastructure, as a subset of the critical infrastructure shares a number of characteristics with its other components (e.g. transport infrastructure or energy networks), but it shows some significant distinctions.

Common characteristics include e.g. the necessity to provide permanent power supply of the key sites, consider impacts of the elements and possible direct threats posed by hostile individuals. With regard to prediction and timely warning against the failure of function delivery the same procedures may be applied as elsewhere.

The question is what may be included into the above mentioned critical information infrastructure? There are mainly data networks, no matter how they are labelled. Central elements, mainly their control, are particularly sensitive sites. Computational systems cannot be disregarded, because they provide users with services (content) without which the significance of networks would not be so high.

Data networks help in daily life, e.g. in cashless payment systems. Longer failure of such systems would make arranging basic necessities of life impossible and would probably require improvised solutions, e.g. in case of food.

3. Resilience and protection of critical information infrastructure

Resilience is the ability to absorb, adapt to and recover fast from the impact of an emergency. Element resilience consists of technical resilience (determined by its robustness and renewability) and organizational resilience (i.e. the processes leading to the strengthening of technical resilience or its adaptability). The element resilience is the higher the lower is the decrease of its performance in the shortest time during an emergency. Vulnerability is the opposite of resilience. Resilience represents internal preparedness of an element for external emergency.

Resistance is the ability of a system to resist threats while maintaining its functionality. Resistance may be perceived also as the ability of a system not to lose its functionality. Infrastructure resistance may be perceived as the ability to reduce the range and time of an emergency. The critical infrastructure resistance is about supplying elementary goods and services regardless an emergency. The efficiency of infrastructure resistance lays in its ability to adapt to or recover fast from emergencies. The resistance of critical infrastructure is an indicator showing the ability to provide the functioning of a system or an element under the impact of external and internal elements. The resistant element provides its target function even under the conditions having degrading effects.

Protection and resilience of critical infrastructure are not contradictory concepts. They represent necessary elements of a complex risk management strategy. Strong foundations built for the protection and resilience of the critical infrastructure remain to be fundamental and decisive part of the risk management in all the areas of critical infrastructure. Suitably determined

impact and sectoral criteria contribute to effective and efficient protection and increased resilience of the critical infrastructure.

The Critical information infrastructure is special by its nonuniformity. Mainly the data networks are operated by many operators, who are in competition with each other. It results in the existence of several parallel area-wide data networks, following their own policies; however, the networks are interconnected in a defined way, e.g. based on the bilateral agreements or in peering centres.

In order to implement security measures in the case when the supply of functions fails, **it is necessary to carry out a rough classification of possible situations** as follows:

- large catastrophe having an impact on a large territory of state, mainly Prague and its surrounding area, where the majority of the network operators are located and the networks are controlled;
- smaller catastrophe having an impact on a part of the state territory;
- cyber attacks against data networks or information systems. Those attacks can be carried out against the networks of one or more operators and may have different goals.

Cyber attacks are special by the fact that **they cannot be specified demographically and their initiators, as well as their purpose are often unknown.** A mere detection is often a problem and includes mainly probes monitoring operation and searching for anomalies.

The issue of cyber attacks **has to be assessed individually** and from different aspect than the above mentioned classical critical infrastructure. The differences are as follows:

- possibility to carry out a massive attack in a few seconds;
- the targets may be area-wide;
- possibility to control key elements unnoticed by their operators;
- possibility to carry out a massive attack from inside the organization;
- the attack itself need not require large resources and may be carried out by individuals with not very high expertise. On the contrary, the preparation of an efficient attack, e.g. searching for weaknesses and vulnerabilities, requires excellent expertise.

It is important to have access to information on the capacity of a network in the real time in order to **build resistant networks**. The information has to be overall, not only from the part of the network. Automated tools should be available and enable comparing the current performance of network with particular metrics or parameters agreed within SLA. The tools should also be capable of determining such situations, which indicate the forthcoming problems.

The most resistant topology is such a topology, in which all the terminal nodes of networks (or the networks themselves) are mutually interconnected. This is the most expensive configuration, though. In practise it is necessary to find such configuration, which balances the cost efficiency and resistance and to provide the systems with the highest capacities of operation with alternative routes, possibly from various providers, being capable of fast activation and the same level of performance.

The resistance of networks can be achieved through the combination of partnerships of service providers, the elaborated design of network, the proactive network management and the recovery programme after an accident. Plans and regular testing are combined with operational philosophy, which connects performance with resistance and resilience capability.

4. Impact and sectoral criteria

Act No 205/2017 Coll. came into effect and amended the Act No 181/2014 Coll. on the Cybersecurity and on the Amendments of Related Acts (Cybersecurity Act), in line with Act No 104/2017 Coll., and other legislation, transposing the Directive (EU) 2016/1148 of the European Parliament and of the Council of July 6 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive). It became mandatory in the above mentioned Act on Cybersecurity to introduce new persons into the system of cybersecurity, i.e. operators of essential services, administrators of information systems of essential services and operators of information systems of essential services.

Act on Cybersecurity entrusts **The National Cyber and Information Security Agency** (NCISA) with the power to assign the operators of essential services and information systems of essential services in the same way as in the case of administrators of critical information infrastructure. The NCISA is empowered by the Regulation to determine the sectoral and impact criteria. The criteria should specify the level of impact the disturbed essential service has on providing the social and economic activities [4].

The National Cyber and Information Security Agency is the central body of the state administration for cybersecurity, including the protection of classified information in the area of information and communication systems and cryptographic protection. It was established on August 1, 2017 based on the Act No. 205/2017 Coll., amending Act No. 181/2014 Coll., on the Cyber Security and on the Amendments of the Related Acts [4].

Chemical industry, medical facilities and gas industry have been beyond the system of critical information infrastructure regardless the cross-cutting criteria set by the government regulation No 432/2010 Coll. on the criteria for determining the element of critical infrastructure. Such a state is unsatisfactory, because information and communication systems in the above mentioned important sectors may cause serious problems both in the cyberspace and real space when ensuring the interests of the Czech Republic. These sectors have been included into a new Directive based on a new NIS Directive. It is necessary to assign

an operator of essential services and define sectoral and impact criteria for each sector.

New regulation shall determine impact and sectoral criteria for determining the operator of essential service and classify the levels of impacts the disturbed essential services have on providing the social and economic activities. It follows the process of determining the cross-cutting criteria according to § 1 of the government regulation No 432/2010 Coll., amended by the Amendment No 315/2014 Coll, and the process of determining sectoral criteria in line with the same government regulation. The reason for such a new regulation is also the obligation of the Czech Republic to implement legal regulations of the European Union, namely **the Directive (EU) 2016/1148 of the European Parliament and of the Council of July 6 2016 concerning measures for a high common level of security of network and information systems across the Union** (the abovementioned NIS Directive). According to Article 5, § 1 of the NIS Directive the EU member states are obliged to identify the operators of essential services in each sector and sub-sector with an establishment on their territory by November 9, 2018 [5].

The sectors and sub-sectors are as follows [6]:

1. **Energy** (The sector of energy is further subdivided into sub-sectors of electricity, oil, gas and heating industry).
2. **Transport** (The sector of transport is further subdivided into sub-sectors of air transport, rail transport, water transport, and road transport.
3. **Health** (The sector of health is not further subdivided, although the NIS Directive includes the sub-sector of health care settings). The sector of health is a newly determined sector and its aim is the effort to increase the protection of health care facilities in the area of cybersecurity and thus reduce the risks, which could limit the functioning of facility and its services and consequently threaten patients´ health and lives.
4. **Water management** (The sector of water management is not further subdivided, although the NIS Directive includes the sub-sector of drinking water supply and distribution, namely the production, supply and distribution of drinking water and wastewaters drainage and treatment. The reason for including this sector on the list is its high dependency on ICT. The aim is to cover all the significant areas of this sector and subsequent population protection and provide people with access to safe drinking water, not harmful to their health. Casualties and the compromising of sensitive personal data are not considered as impact criterion in water management).
5. **Banking** - The aim is to cover significant areas of this sector and increase the protection of credit institutions in the area of cybersecurity. Banking is considered to be a significant sector both in the Czech Republic and the EU and thus the regulation and supervision of this sector is harmonized to a large extent. (The number of clients over 500 000 or the market share exceeding 1 % from the banking sector balance sheet).
6. **Financial market infrastructures** (The sector of financial market infrastructures is not further subdivided). They are the operators of trading venues as defined in the Act on Business Activities on the Capital Market. (6)
7. **Digital infrastructure** (Types of services in this sector include the interconnecting of technically self-sufficient networks, providing services to Domain Name System (DNS) on internet and administration or operation of top-level domain (TLD) name registries. Casualties and the compromising of sensitive personal data are not considered as impact criterion in digital infrastructure.
8. **Chemical industry** (Chemical industry is the only sector the regulation of which goes beyond the NIS Directive. Legislation of this sector stems from the authority awarded to the EU member states to regulate the areas considered to be significant beyond the sectors regulated by the NIS Directive. The types of services in this sector are divided as follows: production of technical gases; production of fertilizers and nitrogen compounds; production of pesticides and other agrochemical preparations; production of explosives; processing of nuclear fuel; production of basic pharmaceutical products; production of other inorganic substances; and production of other basic organic chemical substances). The compromising of sensitive personal data is not considered as impact criterion in chemical industry.

The impact criteria for the above mentioned sectors are perceived as impacts of cybersecurity incidents on information system or network of electronic communications in a given sector on the functioning of which a certain service is dependent. It may cause the following [6]:

- serious limitation or disruption of service affecting more than 50 000 people; or
- serious limitation or disruption of another basic service, or limitation or disruption of operation of the CI element; or
- economic loss higher than 0.25 % of GDP; or
- unavailability of service for more than 1 600 people in the case the service cannot be substituted in another way without disproportionate expenses; or
- over 100 dead or 1 000 injured people requiring medical treatment; or
- breach of public security in a significant part of municipality administrative district which would require rescue and disposal operations carried out by integrated rescue system; or
- the compromising of sensitive personal data on more than 200 000 people (this criterion is not in all sectors considered to be relevant).

5. Personnel

At one hand there is a legislation, legal norms and regulations, but on the other hand it is necessary to have also sufficient number of experts working in the area of critical information infrastructure and its protection. At present there is shortage of experts from the area of cybersecurity in all the required sectors (informatics, information security management, law, etc.). The problem is bigger in public administration, because the public administration cannot pay such experts well. Most experts, graduating from universities in the above mentioned sectors, go to private companies, which can offer them higher salaries and other benefits. The lack of experts may result in employing less qualified personnel and it may then be considered to be a cybersecurity threat, because unprofessional management or interventions into the systems belonging to the CI infrastructure or significant information systems may cause their failure. Lack of experts will necessarily lead to the disproportionate dependence of public administration and its information systems on private companies in the area of the ICT services. It may result in the increased costs of administration and thus the increasing burden for the state budget in relation to such suppliers.

6. Conclusion

It is an elementary task of a state to ensure the protection of critical infrastructure. The state has to ensure that the basic elements, connections and flows of the system within the state will remain operational under normal, abnormal and even critical conditions. Those elements are rudiments enabling the state to be capable of reaching stability and starting further development under any circumstances. Protection of critical infrastructure is part of the crisis management. An element has to meet both the cross-cutting and sectoral criteria to be included into the critical infrastructure. The cross-cutting criteria are a set of general standpoints with limit values determining the seriousness of impact disturbing or destroying the CI element. The sectoral criteria are technical or operational values for determining the CI elements in particular sectors of critical infrastructure. The National Cyber and Information Security Agency assigns the operators of essential services and information systems of essential services in the same way as in case of administrators of critical information infrastructure. For this purpose it determines sectoral and impact criteria in this area. On the grounds of the Directive (EU) 2016/1148 of the European Parliament and of the Council of July 6 2016, concerning measures for a high common level of security of network and information systems across the Union, the EU member states are obliged to identify the operators of essential services in each sector and sub-sector with an establishment on their territory by November 9, 2018. Therefore a draft of the new regulation has been elaborated and discussed in the paper in more detail.

Acknowledgement

This contribution is part of the research project No VI20152019049 called "RESILIENCE 2015: Dynamic Resilience Evaluation of Interrelated Critical Infrastructure Subsystems" granted by the Ministry of Interior of the Czech Republic within the Czech Republic Security Research Programme in 2015 - 2020.

References

[1] Critical Infrastructure and its Protection [online]. Available: http://www.hzscr.cz/clanek/kriticka-infrastruktura-a-jeji-ochrana.aspx [accessed 2017-09-11].
[2] HROMADA, M., HRUZA, P., KADERKA, J., LUNACEK, O., NECAS, M., PTACEK, B., SKORUSA, L., SLOZIL, R.: Cyber Security: Theory and Practice (in Czech). Powerprint, Praha, 2015.
[3] Critical Information Infrastructure [online]. Available: https://www.govcert.cz/download/kii-vis/container-nodeid-663/2schemakii-cz.pdf [2017-09-20].
[4] National Cyber and Information Security Agency [online]. Available: https://www.govcert.cz/cs/ [accessed 2017-09-28].
[5] Act No. 104/2017 Collection of Laws, amending the Act No. 365/2000 Collection of Laws, on Information Systems of Public Administration and on Amendment to Certain Acts, as amended, Act No. 181/2014 Collection of Laws, on the Cyber Security and on the Amendments of the Related Acts (Cyber Security Act), and Certain Acts [online]. Available: https://www.psp.cz/sqw/sbirka.sqw?cz=104&r=2017 [accessed 2017-10-1].
[6] New Cyber Security Notice - Call for Professional Public [online]. Available: https://www.govcert.cz/cs/nova-vkb/ [accessed 2017-10-10].