ADAPTABILITY OF STATE TO A NEW CI CHALLENGES – WITH FOCUS ON CYBER WARFARE DOMAIN

Iztok Podbregar, Polona Šprajc

ABSTRACT: The article presents the current state of the field of regulation of cyber security in the Republic of Slovenia, since the presentation of what cyber security is at all, through the general presentation of individual elements of the Critical Infrastructure Act in the Republic of Slovenia, to the presentation of selected elements of the cyber security strategy in the Republic of Slovenia, which inevitably critical infrastructure. Information security and organizations that ensure the operation of services that fall within the scope of critical infrastructure are a new and essential element of every society and, as such, an exceptionally sensitive topic for the attitude of organizations to service users, on the other hand, a technology-sensitive topic for security issues, which are a key element in assessing the effective and successful handling of critical infrastructure in the country.

KEYWORDS: critical infrastructure, cyber security, law, Republic of Slovenia

1. Introduction

Technology is a tool that in many ways shapes and defines our actions in personal or business life. Technology has evolved as an important part of critical infrastructure through development as it is a key element for each country and citizen from the point of view of organizations that map the development trends of technology into operation, products and services. With the presentation of the importance of information technology, which, together with communication technology, is placed in the top of the importance of protecting and protecting it, the critical infrastructure of the country has been complemented by a set of organizations that we are pursuing and needed in this context. Because the world is surrounded by diverse challenges as well as threats, the world of information and communication is all the more exposed to situations that a normal individual can instantly turn to the opposite position from the position that an organization or state wants. Knowledge and management of situations that in the world of the Internet essentially mean an intangible picture of the transmission of information and data can at some point be extremely critical and also point out the life threats of individuals or a larger group. For this purpose, the contribution is also aimed at presenting the key information security positions, which should not remain somewhat behind but something that must be, but it is an area that must be managed and developed with the most precise protection technique, on the

one hand, of such an intangible nature, on the other hand, because technology nowadays in many ways creates our actions and actions and generates decisions that often have a key effect on the success and effects of our lives.

2. What is Cyber security?

Cyber security is generally defined as (Digital Slovenia, 2017):

a) a set of activities and other measures, both technical and non-technical, intended to protect computers, computer networks, hardware and software, and information provided by them contains and treats, which includes software and data as well as other elements cyber space, against all threats, including threats to national security;

b) the degree of protection that the activities and measures can provide;

c) pooled areas of professional effort, including research and development in the field implement and improve measures and raise the quality of these measures.

According to SI-CERT data, 2060 incidents were reported in Slovenia in 2014, which is almost a 6.4 % increase compared to 2008 (Digital Slovenia, 2017).

The growing trend with regard to the above-mentioned malnutrition of the cyber-security system is of concern (Digital Slovenia, 2017).

The SI-CERT (Slovenian Computer Emergency Response Team) is the national response center for dealing with incidents in the field security of electronic networks and information, which has been operating within the Arnes public institute since 1995. It coordinates incident incidents, technical advising on intrusions, computer infections and other abuses, and issuing warnings for network managers and the general public on current threats in electronic networks (Digital Slovenia, 2017).

Despite the fact that cyberattacks are occurring with greater frequency and intensity around the world, many either go unreported or are under-reported, leaving the public with a false sense of security about the threat they pose and the lives and property they impact. While governments, businesses and individuals are all being targeted on an exponential basis, infrastructure has become a target of choice among both individual and state-sponsored cyber-attackers, who are targeting security systems that were previously thought of as impenetrable. This has served to demonstrate just how vulnerable cities, states and countries have become, and the growing importance of achieving global risk agility in the face of such threats (https://intpolicydigest.org/2018/03/25/cyberwarfare-against-critical-infrastructure/).

3. **Law and Regulation in the Republic of Slovenia (Uradni list RS, 2017)**

The purpose of the Critical Infrastructure Law (2017) is to systematically regulate the continuity of the critical infrastructure. Its

protection covers all activities that contribute to the continuity and integrity of its operation.

The Law includes different categories of critical infrastructure: water, food and energy supplies, health care, the financial sector, transport, environmental protection and the information and communication systems and networks sector are defined for the critical infrastructure sectors.

Sector holders are ministries responsible for the areas of work to which critical infrastructure belongs, and the Bank of Slovenia.

The law determines the systemic foundation of the critical infrastructure area from its identification and determination to its protection, which is reflected in the main solutions of the law.

The objectives of the law are, in particular, to regulate (also) the area of critical infrastructure of national importance, that is, the "national" critical infrastructure, and by means of a normative measure, it contributes to raising the level of resilience of Slovenian society against modern security threats and risks.

Organizations

In order to ensure the continuity and full operation of critical infrastructure, all bodies and organizations are required to respect the same general principles and guidelines.
Appropriate relationships are established between bodies and organizations operating in the areas of critical infrastructure sectors, in particular in terms of sharing their

responsibilities and responsibilities and tasks in protecting critical infrastructure.

The Role of Government

The government is the highest state body that defines, directs and coordinates the policy in the field of critical infrastructure.

Regardless of the ownership structure of the critical infrastructure, the operators and owners of critical infrastructure are first and foremost responsible, and also interested in the business of ensuring critical operation of the continuous operation of the critical infrastructure.

Control

Supervision over the implementation of the provisions of the law will be carried out centrally through the inspectorate responsible for defense, but this does not exclude the possibility that in accordance with existing regulations and established working methods for inspectorate, the said inspector will also attract other inspection bodies with real competences in the area of the critical infrastructure sector under which surveillance is carried out.

The Measures

The measures for the protection of critical infrastructure are divided into permanent and additional.

Additional measures are carried out in the event of an emergency, crisis, or increased threat to critical infrastructure, if permanent, even if they are graduated, are insufficient.

Additional measures for the protection of critical infrastructure that are adopted by the Critical Infrastructure Sector institutions themselves or proposed for adoption by the Government are not mandatory, as they can be accepted or proposed by the institutions only if they deem it necessary.

Communication

The law also defines, inter alia, obligations regarding information, reporting and provision of decision support in connection with the provision of the continuous operation of critical infrastructure.

4. **Principles of Critical Infrastructure Protection (Uradni list RS, 2017)**

   a) **The principle of an integrated approach** requiring that all critical authorities and organizations are involved in the protection of critical infrastructure before and during interruptions in the operation or interruption of critical infrastructure operation, and taking into account the different types of hazards derives from the risk assessment and takes into account the interdependence of the critical infrastructure sectors and their interaction.

   b) **The principle of responsibility** for which Critical Infrastructure Managers are directly responsible for the operation of Critical Infrastructure and all competent authorities and organizations to strengthen Critical Infrastructure Protection.

   c) **The principle of protection against different types of hazards**, which requires

that all competent authorities and organizations take into account different types of natural and technological threats in ensuring the critical operation of the critical infrastructure.

d) **The principle of the ongoing planning of critical infrastructure protection**, which requires that the planning of critical infrastructure protection is supported by a continuous process of assessing the risks to the operation of critical infrastructure and assessing the appropriateness of the measures for its protection.

e) **The principle of data and information exchange and data protection**, which requires regular, timely and trusted exchange of data and information from all competent authorities and organizations, while protecting data related to critical infrastructure, in accordance with the regulations governing the protection of classified information or business secret.

5. Cyber Security Strategy in the Republic of Slovenia (Digital Slovenia, 2017)

With this strategy, Slovenia delfine measures to establish a national cybernetic system security that will be able to respond rapidly to security threats and will provide effective protection information and communication infrastructure and information systems, which will be provided with the continuous operation of both the public and the private sector, and in particular the key functions of the state and companies in all security conditions.

Ensuring the safety of cyberspace will be balanced between the interests of ensuring security and economic viability and human rights, and fundamental freedoms.

5.1 Goal of strengthening and systemic regulation (Digital Slovenia, 2017)

In order to achieve the goal of strengthening and systemic regulation of the national cybernetic system security measures are taken:

- the establishment of a central coordination of the national cyber security system;
- staffing and technological strengthening of organs at the operational level of the cybernetic system security together with the establishment of SIGOV-CERT;
- regular participation in international exercises in the field of cyber security and carrying out national exercises;
- gradually upgrading the network of HKOM national authorities with equipment duly certified by the parties' Slovenian authorities as safe and suitable for use;
- establishment of competent certification of the security and functionality of information equipment in existing and newly established bodies.

5.2. Goal of citizen's safety (Digital Slovenia, 2017)

In order to achieve the goal of citizens' safety in the cyberspace, measures are implemented:

- the regular implementation of awareness-raising programs in the field of cyber security;
- introduction of content from the field of cyber security into the education and training system.

5.3 Goal of cyber security in the economy (Digital Slovenia, 2017)

In order to achieve the objective of cyber security in the economy, measures are implemented:

- promoting the development and introduction of new technologies in the field of cyber security;
- the regular implementation of awareness-raising programs in the field of cyber security for economic subjects.

5.4 Goal of ensuring the operation of critical infrastructure in the ICT sector (Digital Slovenia, 2017)

To achieve the goal of ensuring the operation of critical infrastructure in the information and communication sector support is implemented:

Regular assessment of the risks to the operation of the critical infrastructure of the information and communication sector support, planning appropriate measures to protect and update the assessment risks in this field.

5.5 Goal of providing cyber security in the field of public security (Digital Slovenia, 2017)

To achieve the goal of providing cyber security in the field of public security and repression cybercrime measures are implemented:

- Implementation of appropriate cybernetic capabilities to protect information and communication police systems;
- regular training in cyber security for law enforcement agencies involved in development cybernetic capacities in the field of public security and in the suppression of cybercrime;
- regular updating of legislation and procedures in line with the development of information and communication technologies.

5.6 Goal of developing defense cyber capacities (Digital Slovenia, 2017)

In order to achieve the goal of developing defense cyber capacities, a measure is implemented:

development of appropriate cybernetic capabilities for defense of defense communications and information systems.

5.7 Goal of ensuring the safe operation and availability of key information communication systems (Digital Slovenia, 2017)

To achieve the goal of ensuring the safe operation and availability of key information communication systems in case of major

natural and other disasters, a measure shall be implemented:

Ensuring the conditions for the smooth operation of key information and communication systems at major natural and other disasters.

5.8 Goal of strengthening national cyber security (Digital Slovenia, 2017)

To achieve the objective of strengthening national cyber security with international cooperation is carried out action:

Providing conditions for the participation of Slovenian experts in relevant international work bodies and associations in the field of cyber security.

6. Conclusion

Our lives are often in the hands of someone who we are not and will never have the opportunity to meet. Virtual reality, robotics, the virtual world are just a few elements that are no longer so coincidental with our everyday life. Our day-to-day decisions, the operation we perform through seemingly secure Internet environments, can be overcome in a severe distress or problem in case of poor protection of the individual or the state. Critical infrastructure, in terms of technology, information and communications development, is far more than just another area that the state must protect as a puncture of its eye. Precisely because of the extreme dimensions, where boundaries, laws and rules often lose significance precisely because of the virtually of the technology process, defining frameworks within strategies

is all the more decisive for the possibility of protecting each individual. Interestingly, the more we see the novelty that enriches our lives, the more fear we fear of situations that are more or less unknown to us - precisely because of the space of the dimension that the world of communication and information offers. In order to create a safe environment, it is therefore important to draw attention to such contributions and to remind us of situations and opportunities that operate within the state, and represent the elements of safe and bold behavior of organizations in the specific framework of the country's infrastructure.

References

1. *Digital Slovenia. (2017). Cyber Security Strategy. Republic of Slovenia.*
2. *International Policy Digest. (2018). Cyberwarfare against Critical Infrastructure. Received May 12 2018 from https://intpolicydigest.org/2018/03/25/cyber warfare-against-critical-infrastructure/.*
3. *Uradni list RS. (2017). Zakon o kritični infrastrukturi. Republic of Slovenia.*