VIII INTERNATIONAL SCIENTIFIC PROFESSIONAL CONFERENCE
SECURITY AND CRISIS MANAGEMENT – THEORY AND PRACTICE (SeCMan)
-SAFETY FOR THE FUTURE-
29th and 30th September 2022, Sremska Kamenica, Republic of Serbia

CHALLENGE RISKS AND THREATS TO INFORMATION SECURITY

Hatidza Berisa[1], Tamara Gajic[2], Jovan Prelic[3]
[1] University of Defence in Belgrade, National Defence School, Veljka Lukica-Kurjaka Street No. 1, Belgrade, Republic of Serbia, hatidza.berisa@mod.gov.rs
[2] J-6, General Staff of the Serbian Army, Belgrade, Republic of Serbia, tamara.gajic@vs.rs
[3] University of Defence in Belgrade, National Defence School, Veljka Lukica-Kurjaka Street No. 33, Belgrade, Republic of Serbia, jovqan.prelic@mod.gov.rs

Received: 14th July 2022
Accepted: 24th September 2022

Professional paper

Abstract: *Extremely rapid scientific and technological development, the diffusion of modern scientific achievements and technology and their growing impact on all areas of social life in countries around the world increase the complexity of the strategic environment. In this context, there will be greater potential for achieving a positive impact on the economic development of countries, through the application of innovative technological solutions that will contribute to improving the use of resources and accelerated productivity growth.*
Systems based on information and communication technologies are another subsystem of the strategic environment whose task is to manage information or uncertainty and thus improve and accelerate the decision-making process. However, they also significantly affect other characteristics of the strategic environment, making it more dynamic, complex, unstable, nonlinear, and especially uncertain.
The authors start from the rapid scientific and technological progress, which causes various dangers, so the focus is on possible challenges and risks, which are manifested through the threat to information security.

Key words: *security, social life, technology, information, information security*

1. INTRODUCTION

The need to know the environment as well as the certainty of what will happen in the future forced man, from its inception until today, to collect data from them, draw the necessary information and then learn and think about how to achieve the set goals. As man became aware of his environment, his need for additional knowledge grew, which necessarily led to the development of both society and various scientific fields. Through its development, human society has gone through various stages, given the amount of information that is now available to us, and that we need, we can say that we live in an information society. The development of information technologies, networking and the global computer network have made real-time information available to us from anywhere in the world.

Today, IT equipment and access to high-speed Internet are available to the majority of the population at very reasonable prices, so that users whose IT knowledge is modest can perform various activities on the Internet from their home, street or other place where the Internet is available. They can establish video communication, make money transactions, monitor the movements of their children and monitor the house and household appliance. Through social networks, they can express their views on various issues as well as comment on the views of others; they can work and learn from home, they can access various Internet presentations and databases. Also, in order to optimize business processes, most public and private companies perform certain business processes from remote locations using information and communication technologies. These can be tasks such as control and supervision of fuel tanks, management of locks, control and supervision of the power system, traffic management, health information systems, banking information systems, command information systems and others. In these activities on the network, a huge amount of data is recognizable, which is exchanged between network communication devices through various telecommunication channels and can be the subject of abuse.

In just one human generation, information and communication technologies have revolutionized the way we live, learn, work and have fun. Information and communication technologies are increasingly transforming the way people, companies and public institutions (Strategija razvoja informacionog drustva u Republici Srbiji do 2020. godine) interact, at the local, regional and global levels. In addition to orientation in a strategic environment, the goal of information is continuous progress, which can only be achieved if you have the necessary knowledge with the application of strategic thinking. The mere possession of modern technologies without the necessary knowledge and awareness of their use, shortcomings and shortcomings necessarily lead the system to ruin with inestimable damage. In addition to space and time, speed is another quantity in a strategic environment, the limits of which one cannot see at this stage of development. The speed of information flow ensures timely and accurate manifestation of the effects that change the strategic environment. Some systems in a strategic environment are not able to keep up with rapid and imposed changes, which put them in a state of general insecurity and danger to survival. However, contrary to expectations that the level of responsibility of all involved entities will be increased in terms of using scientific achievements in the general interest and for the benefit of all mankind, it is estimated that the development of science and technology will continue to be subject to various abuses (Tatomir, 2018).

Given the importance of information and information power in the strategic environment, the fact arises that information security is key to achieving strategic goals (Berisa, 2016). Recognizing the benefits of information and communication technologies, the security of personal information becomes very important for the security of every individual in society.

The Republic of Serbia has recognized the need to improve the security of citizens, the state and society and through the National Security Strategy has set priorities: "In the field of cyber security warfare in the information and cyberspace. Significant attention will be paid to the further development of the general security culture of all citizens in order to raise awareness of the need to increase the security of individuals and society (Nacionalna strategija odbrane u Republici Srbiji, 2019).

2. CONCEPT AND DEFINITION OF INFORMATION SECURITY

In theory and practice, we encounter concepts such as: data protection, information security, information security, information protection, cyber security and others. The definition of these terms usually depends on the degree of scientific and technological development of the country at the time when it was created as well as the context of the definition. It is a common

occurrence that, given the rapid technological development and coverage of information and communication technologies, the definitions of these terms have changed several times in a very short period of time.

In the last decade, the terms information security and cyber security have often been used interchangeably. However, considering the environment of action, it is considered that there is a difference between them, which leaves room for further development of scientific discussions. In order to better understand and reflect on this problem, it is necessary to consider Figure 1. In general, looking at all information, we can divide it into analog and digital, with the development of information and communication technologies, there is an increasing digitalization and translation of analog into digital information. (Explanation: Digital information can be considered information that is transmitted, stored or processed using information and communication technologies, ie information that is used to manage and use (software) other systems (hardware) also using information and communication technologies. While we consider all other information as analogous). If we consider the data in a certain context, it becomes information and gets a higher value, so in certain circumstances, and especially if it is about national security, it needs to be protected. In terms of security threats, information is the most common means by which a goal is reached, so that its value also depends on the value of the goal.

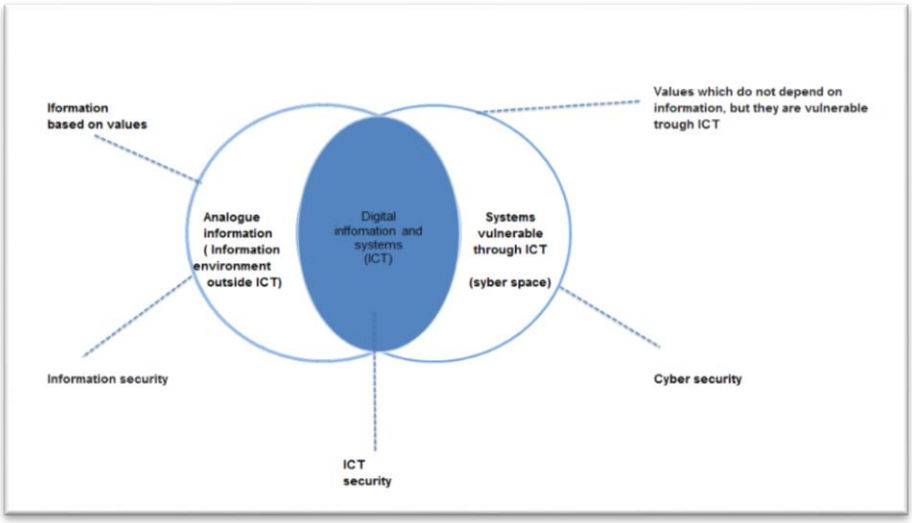

Figure 1: Relationship between information, ICT security and cyber security
Sourse: (Mladenovic, 2016)

Looking at Figure 1, we can conclude that information security refers to the protection of information and information in ICT systems, cyber security refers to systems that are vulnerable through ICT systems, while ICT security refers to the protection of ICT systems. According to the Law on Information Security, the information-communication system (ICT system) is a technological-organizational unit that includes: electronic communication networks; devices or groups of interconnected devices; data that is kept, stored, processed, searched; organizational structure through which the ICT system is managed and system and application software.

However, it is difficult to imagine a system that does not depend on information, and thus on information security, without being vulnerable through the ICT system. In a general sense, information security is a more general term and refers to analog and digital information, while

cyber security refers to the protection of values that can be violated through digital information. Information and cyber security should therefore not be viewed in the relation of a subset to a set, but as a relation of two different systems of reality, of which cyber security has an additional dimension related to the protection of security features and other information resources (The concept of cyber defense of the Serbian Army, 2018).

In the Law on Information Security, information security is defined as a set of measures that enable data handled through ICT systems to be protected from unauthorized access, as well as to protect the integrity, availability, authenticity and irrefutability of that data in order for that system to function. Availability is a property that means that data is available and usable at the request of an authorized person when they need it. Authenticity is a property that means that it is possible to verify and confirm that the data was created or sent by the person for whom it was declared that he performed that action. Irrefutability is the ability to prove that a certain action has taken place or that a certain event has occurred, so that it cannot be subsequently denied. Provided, when provided and under the control of an authorized person. A very important property of data or information is secrecy, which means that the data is not available to unauthorized persons. Depending on the value that is protected, the degree of secrecy is determined, and thus the level of security protection.

The most common international standard ISO / IEC 27000 defines information security as: preserving the confidentiality, integrity and availability of information, noting that other properties, such as authenticity, responsibility, non-repudiation and reliability may be included (ISO/IEC 27000:2018(en)). Information security is a very important segment of national security which provides secure and uninterrupted communication, storage, transmission and processing of data of state bodies and other subjects of social life in performing activities to preserve national values and achieve national interests. Information security is also the right of every citizen to inviolability and secrecy of communication as protection of personal data.

3. NORMATIVE AND LEGAL FRAMEWORK IN THE FIELD OF INFORMATION SECURITY

Twenty years after the connection of the Republic of Serbia to the global computer network, in 2016 the Law on Information Security was adopted, which, together with the Law on Ratification of the Convention on High-Tech Crime from 2009, represents the legal framework in this area. The adoption of the Law on Information Security is also envisaged by the negotiating Chapter 10. Information Society and Media in the Process of Accession of the Republic of Serbia to the European Union, but also by the Strategy for the Development of the Information Society until 2020. In 2017, the Government of the Republic of Serbia adopted the Strategy for the Development of Information Security in the Republic of Serbia in the period from 2017 to 2020, which defines the key directions and goals of action in the field of information security. The mentioned strategy envisages five priority areas, of which the fourth Information Security of the Republic of Serbia is given to the Ministry of Defense. An Action Plan for 2018 and 2019 was adopted to implement the strategy.

The Law on Information Security envisages the establishment of the Team for Coordination of Information Security Affairs in order to achieve cooperation and coordinated performance of tasks in the function of improving information security. The team includes, among others, representatives of the Ministry of Defense and the security services. It is also envisaged to establish the National Center for Risk Prevention in the ICT System of the Republic of Serbia (National CERT) as well as CERT authorities, independent operators of ICT systems and special CERTs. The National CERT performs the tasks of coordination of prevention and protection against security risks in ICT systems at the national level, while other CERTs perform the tasks of prevention and protection against security and risks in ICT systems in

their jurisdiction. The Ministry of Defense and security services, as independent operators of the ICT system in terms of the Law on Information Security, have the obligation to establish CERT.

The Ministry of Defense and the Serbian Army, following the normative legal regulations of the Republic of Serbia, have so far developed the Concept of Cyber Defense of the Serbian Army, Instructions on ICT System Security in the MoD and Armed Forces, Instructions on Using the Computer Network of MoD and Armed Forces Commands, and VS as well as through procedures related to information security. In addition to the above documents, the legal framework in the field of information security is regulated by the Law on Critical Infrastructure, the Law on Electronic Communications, the Law on Data Secrecy, the Law on Personal Data Protection, the Criminal Code and other laws and legal acts.

Knowledge and application of the international standard ISO/IEC 27000 is also important. This standard provides a series of best practice recommendations on information security management. It is applicable to organizations of different shapes and sizes, encourages organizations to assess information risks and to control them in accordance with their needs. The organized process of building the operational and legal framework of information security has begun, and the adopted laws represent a good foundation for further improvement of information security. This process will take place through the development of digital culture of all citizens, continuous monitoring of contemporary ICT and training of professional bodies, application of international standards, application of practical experience, continuous development of information security systems at the legal, organizational and technical level and risk assessment and information security threats.

4. METHODOLOGY OF PERFORMING RISKS AND THREATS TO INFORMATION SECURITY

Given the complexity of the strategic environment, it is not possible to provide full protection of information, awareness of the challenges, risks and threats to information security allows us to manage risks and act preventively on potential threats. Based on the insight into numerous researches of the concept of security and its content, a significant discrepancy is noticed about what is specifically meant by security risks. The persistence in practice that this term is most often used simultaneously with the term challenge and threat creates a basic dilemma regarding their definition as synonyms or terms of different levels of generality (Tatomir, 2018). A challenge, as a concept of a higher level, refers to a phenomenon or process that is possible and probable, initially indefinite and value-neutral. If a negative value prevails, the challenge becomes a risk and the probability of adverse impact on a particular security facility gradually increases. Risk is a notion of a lower level of generality than a challenge and can be defined as a possibility, i.e. as a certain degree of probability of occurrence of an event or action with unfavorable consequences, where its elimination or reduction depends on the level of knowledge of the phenomenon.

The international standard ISO / IEC 27000 defines the risk to information security as the potential by which a given threat will exploit the vulnerability of an asset or group of assets and thereby harm the organization. According to the Law on Information Security, risk means the possibility of violating information security, i.e. the possibility of violating the secrecy, integrity, authenticity or inviolability of data or disrupting the direct functioning of the ICT system. A threat is, in the broadest sense, a conscious intention to cause damage to a value. According to the international standard ISO / IEC 27000, a threat is a potential cause of an unwanted incident, which can lead to damage to the system or organization. Information security threats are most often related to the vulnerabilities of an ICT system or organization.

Information security risk management should be an ongoing process. The process begins with establishing an internal and external context, followed by risk assessment, risk management, and risk acceptance. During the process, the risk is continuously monitored and reviewed with constant communication and consultation regarding the risk. In this part of the security risk management process, we can recognize the role of CERTs.

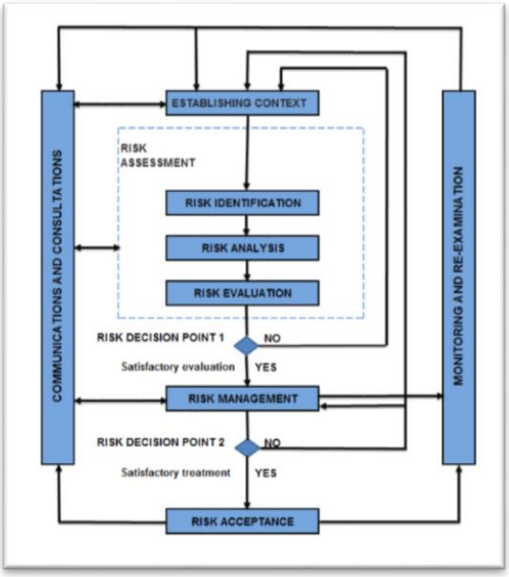

Figure 2. Information security risk management algorithm
Sourse: (Information security risk management ISO/IEC 27005:2017)

As shown in Figure 2, the information security risk management process can be repeated to assess risk and risk management activities. The repetition of the risk assessment and management process deepens and increases the details in the risk management approach itself. The establishment of the internal and external context for information security risk management implies the setting of the necessary criteria for risk evaluation, the criterion of the impact of risk on the system or organization and the criterion for risk acceptance. Next, it is necessary to determine the subject and area of application, i.e. to define all values / assets that are taken into account when assessing the risk and to determine the limits so that we can identify where the risk comes from. When we say assets that means Values or assets in terms of information security include business processes and activities, information, hardware, software, networks, staff, location and structure of the organization. A very important part of this phase of the process is the establishment and maintenance of the organization and responsibility for information security risk management.

Information security risk assessment is the second phase of this process and includes the following steps: risk identification, risk analysis and risk evaluation. Risk identification is a comprehensive and detailed process that should determine the events that may lead to potential damage as well as to determine how, where and why the damage may occur. Risk identification includes detailed identification of assets, identification of threats, identification of existing controls and identification of consequences. Risk analysis is conducted for varying degrees of detail, depending on the criticality of the asset, the extent of known vulnerabilities, and previous incidents that have occurred in the organization. It is realized through the assessment of the consequences and probability of the occurrence of incidents. The last step in this phase

is risk evaluation, which is a procedure in which the level of risk should be compared with the criteria for risk evaluation. At the end of this phase, a list of risks ranked by priorities is obtained; the assessment can be conducted in several repetitions.

Dealing with information security risk is a procedure where by taking appropriate measures, in an economical and efficient way, the existing risk is affected so that it becomes acceptable. There are four non-mutually exclusive risk management options: risk modification, risk retention, risk avoidance and risk sharing. If the risk management is not satisfactory, it is possible to return the process to the beginning or to the risk management again.

Risk acceptance is often not a simple determination of whether residual risk is within the criteria for risk acceptance. In some cases, it is necessary to return the criterion for accepting the risk of finishing. Communication and consultation on information security risk are activities that are agreed upon on how to manage risk. Effective communication is very important and can significantly influence decision-making; it takes place in two directions between all stakeholders. Monitoring and reviewing information security risks are an essential activity to identify any changes in the environment that affect existing risks and values. Risks are part of the environment and in that sense you are not static, their nature is dynamic, non-linear and it is necessary to constantly monitor them. The mentioned methodology can be applied to organizations and systems of different shapes and sizes, as well as to their individual parts. Risks and threats to the system and organization in terms of security of information by origin can be divided into deliberate cyber-attacks, accidental and natural. If intentional risks and threats are identified in the digital information environment or cyberspace, then we call them cyber attacks but the cause of natural disturbances is not a human factor but natural phenomen

Some of the possible threats that could worsen information and the ICT system are:

- Physical damage due to: fire, flood, earthquake, etc. ;

- Interference due to different types of radiation such as: compromising electromagnetic radiation , other electromagnetic radiation, electromagnetic pulse, etc.

- Compromising information such as: signal interception, eavesdropping, theft of documents or media, position detection, accidental or intentional disclosure, data from untrusted sources, manipulation of hardware and software, etc. .;

- Technical failures such as hardware and software failure, power failure, etc. .;

- Unauthorized actions such as: unauthorized copying of software, unauthorized use of equipment, use of counterfeit software, unauthorized intrusion into the system

The most common sources of intentional human threats to the security of information and ICT systems are: hackers, computer criminals, terrorists, spies and insiders. Motivation for their activities can be: money, status, ego, rebellion, revenge, political gain, competitive advantage, curiosity, deliberate destruction of information, etc.

These are just some of the possible risks and threats that are always related to the vulnerabilities of the system and the organization and they can be the following:

- Hardware: poor quality of equipment, poor maintenance, lack of periodic replacement, lack of available protection, etc.;

- Software: absence or insufficiently tested software, wrong access rights, lack of documentation, non-logging out or leaving the workstation, incorrect dates, complicated user interface, widely distributed software, lack of backups, etc.;

- Network: unprotected and unreliable communication lines, poor connectivity, poor network management, only network monitoring, unprotected public connections, etc.

- Staff, lack of staff, insufficient training, lack of security awareness, inadequate selection of staff, lack of monitoring mechanisms, etc. .;

- Location: lack of physical protection of the building or room, unstable electrical network and fire protection, etc. ;

Organization: lack of plans, policies and procedures, lack of control and verification, etc.

From all the above, it can be seen that risk management for information security is an extremely complex and continuous process of influencing risks in order to provide conditions for the organization to achieve the set goals in an efficient and economical way. The number of possible risks and threats is practically unlimited and is directly linked to system vulnerabilities. Through creative and critical thinking, it is possible to analyze and evaluate those risks and threats that must be addressed in order to ensure the functioning of the organization.

5. CONCLUSION

Considering the overall state of information security in the Republic of Serbia, it can be concluded that the process of institutionalization of this area is very slow. It seems that the foundation of the normative-legal framework was adopted with a considerable delay more as an obligation arising from the accession negotiations with the European Union and not as a need to establish an information security management system as one of the important elements of the national security system. The state of information security in the MoD and the Armed Forces is at a slightly better level, the use of a closed computer network with crypto security and defined security procedures in terms of staff selection, security and more, significantly reduces the possibility of information security breaches.

However, the level of information security is not satisfactory and requires additional efforts. It is noticeable that the normative legal framework has been formed in accordance with international standards and that such practice should be continued in the development of documents that regulate this area at the operational level. The stated methodology of risk management for information security is applicable to the mobile and stationary element of the telecommunication-information system of the MoD and the Armed Forces in peace, war and state of emergency. During 2020, the backbone of the administrative body for information security and cyber defense was formed in the Directorate for Telecommunications and Informatics of the General Staff of the Armed Forces, and it is expected that in the coming period there will be the formation of administrative bodies at the operational level. MO and VS. However, without the understanding and support of the responsible persons in managerial positions in the MoD and the Armed Forces, who should provide funds for the development of the necessary capabilities, it is not realistic to expect a significant improvement in information security. Also, a very important factor is the development of digital culture at the national level as well as raising awareness of all members of the MoD and the Armed Forces about the importance of information security. We live in a real cyber environment of the digital society, enjoying all its benefits but with an insufficiently built awareness of the risks and threats it carries. It is high time that we take responsible measures in order to protect national security and thus the security of citizens in cyberspace. The possibilities brought by the use of modern information and communication technologies to achieve positive or negative effects in a strategic environment are the greatest challenges of humanity at the beginning of the 21st century.

REFERENCES

Action plan for 2018 and 2019 for the implementation of the strategy for the development of information security in the Republic of Serbia for the period 2017-2020. year, "Official Gazette of RS", no. 14 of 23 February 2018.

Berisha H, Barisic I. Security challenges cyberspace and information warfare, Regional Scientific and Professional Conference ZITEH-16: Information Technology Abuse and Protection, June 1, 2016, Belgrade,

Concept of cyber defense of the Serbian Army, Belgrade: Directorate for Training and Doctrine (J-7) of the General Staff of the Armed Forces, 2018

Information Security Development Strategy in the Republic of Serbia for the period from 2017 to 2020, "Official Gazette of RS", no. 53 of 30 May 2017

Information security risk management ISO / IEC 27005: 2017

Instruction on the security of ICT systems in the MoD and the Armed Forces, "Official Military Gazette", No. 24 of September 20, 2019

International Organization for Standardization / International Electrotechnical Commission. (2018). Information technology - Security techniques - Information security management systems - Overview and vocabulary (ISO / IEC 27000: 2018)

Mladenovic D, "Multidisciplinary aspects of cyber warfare", Doctoral dissertation, Faculty of Organizational Science

Nacionalna startegija odbrane Republike Srbije, Sluzbeni glasnik Republike Srbije, br. 94/2019.

Strategija razvoja informacionog drustva u Republici Srbiji do 2020. godine, Sluzbeni glasnik Republike Srbije, br. 51/2010,

Tatomir, D., "Assessment of challenges, risks and threats to the security of the Republic of Serbia in the function of planning the use of the Serbian Army", Vojno delo, spring 2011.

Zakon o elektronskoj komunikaciji, Sluzbeni glasnik Republike Srbije, br. 5/2018.

Zakon o kriticnoj infrastrukturi, Sluzbeni glasnik Republike Srbije, br. 87/2018.

Zakon o tajnosti podataka, Sluzbeni glasnik Republike Srbije, br. 104 /2009.

Zakon o zastiti informacija, Sluzbeni glasnik Republike Srbije, br. 6/2016 2016