Cybersecurity Management at National Level

George Daniel ȘAPERA
National Institute for Research and Development in Informatics – ICI Bucharest
george.sapera@ici.ro

Abstract: The article highlights the key role of cyber research, stressing the need to focus efforts in the context of determining the manner in which the key actors should reach a common understanding of how to design and respond to security challenges in cyberspace. In order to build a clear perception of these effects, the article addresses the main elements defining cyberspace that support the efficiency of the management process, especially when we speak of cyberspace as an area of economic, political and military conflicts. The discussion on national critical infrastructure protection is increasingly focused on the cyber dimension, as all infrastructures are affected by the information revolution and include IT components, mainly for command-and-control functions.

Keywords: Cybersecurity, Critical infrastructure, Management, Cyber risk.

INTRODUCTION

We live in an increasingly interdependent world, and this is largely due to the evolution of Information and Communication Technology (ICT). There are many benefits stemming from this interdependence, but many disadvantages as well, given that the most advanced public institutions and businesses have become critically dependent on the reliable, accurate and continuous functioning of such systems, with little redundancy and alternative. Governments around the world need therefore to be prepared for a new set of challenges, when national economies, national security and the daily life of all citizens depend on a safe and stable cyberspace.

The process of globalization has led states to relinquish their absolute sovereignty, moving to accepting alliances or influences from international organizations.

Now, the facilitated access to technological developments and their increase in size, complexity and influence provide the opportunity for non-state entities to become leading actors. The emergence of these actors, who have profited from the spread of state-of-the-art technologies and have moved to the technological vanguard, has led to an increased uncertainty and to structural transformations potentially affecting national security interests, such as the increased reliance on private contractors in intelligence work.

The dramatic events in the US (on September 11, 2001), as well as in Madrid (on March 11, 2004) and in London (in July 2005) have confirmed that modern societies are increasingly vulnerable to terrorist attacks and asymmetric threats. They target the safety of persons and the security of infrastructures which are essential for the proper functioning of the society as a whole.

The revealed scale of these threats alarmed decision-makers as they calculated not only the risks to national security but also the significant human, financial and material implications. This is nowhere more evident than in cybersecurity, where attackers started out with viruses created for fun and ideology, and have ended up with complex products used for industrial espionage, for targeted sabotage and for large scale disruption, under coercion.

The security events that followed have led to the awareness of the seriousness of a cyber threat. In 2007, Estonia was affected by a cyber-attack on public authorities, banks and many companies. During the Russian-Georgian conflict in August 2008, massive attacks were launched on government sites and servers in Georgia, illustrating the term “cyber war”.

However, the real start of the cyber war can be dated in 2010 with the emergence of the first cyber-weapon, the STUXNET virus, designed to take control of and subtly sabotage a state’s critical infrastructure (Monitor, 2010).

In the following years, the number of cases of cyber-attacks has increased, with a significant impact on national security. This dynamic and complex environment, which is constantly evolving, must be regulated, without affecting the fundamental rights and freedoms of citizens, as well as their potential for development.

ROMANIA’S CYBER CAPABILITIES

In the context of maintaining and developing an effective approach to national security, Romania has established guidelines for cybersecurity in order to protect its communication systems and reduce risks to the Alliance, and it has also moved to implementing specific tasks deriving from NATO’s cyber defense policy. Efforts to establish the Cyber Security Guidelines have been crowned with the government approval on the Cyber Defense Strategy and the national Action Plan on the implementation of the National Cybersecurity System (Monitor, 2013a) through Government Order 271 of 23 May 2013.

According to the Strategy, the National Cybersecurity System (NCS) is the overall framework for cooperation, bringing together public authorities and institutions with responsibilities and capabilities in this area, with a view to coordinating national action to ensure cybersecurity. It features knowledge, prevention, cooperation, coordination and counterbalanced components. The authority that coordinates the activity of the NCS at strategic level is the Supreme Council for National Defense (Monitor, 2015).

The body through which security is coordinated is the Computer Security Operational Council – COSC, which includes representatives of the Ministry of National Defense, the Ministry of Internal Affairs, the Ministry of Foreign Affairs, the Ministry of Communication and Information Society, the Romanian Intelligence Service, the Special Telecommunications Service, the Foreign Intelligence Service, the Security and Guard Service, the Office of the National Register for State Classified Information, as well as of the Secretary of the Supreme Council for National Defense. The COSC technical coordinator is the Romanian Intelligence Service.

Each institution represented in the COSC cooperates with the international bodies of the EU, NATO, OSCE, etc., in its area of competence. Now, at global level, public and private organizations from various sectors identify cyber-attacks as one of the most widespread and high-level risk they face.

Addressing cyber threats is a complex challenge. Most actions now address protection and compliance measures, as organizations are subject to increasing legislative and regulatory requirements and aim to demonstrate that they can manage and protect their information and systems properly. The information security area is constantly evolving. Public and private sector organizations are reluctant to accept that they may be the target of cyber-attacks. This mentality must evolve, although there are still important ethical and legal constraints on such an approach. At the same time, only the defense strategy is no longer viable. A determined opponent will finally manage to reach his goal. As a result, public and private sector entities need situational awareness to know when an attack occurs or if it is imminent. Information collection and analysis and control possibilities will be the basis of the new generation of information security solutions (Monitor, 2013b).

Cyberspace has achieved a global level of operation for everyone, from users to corporations and governments, and it is increasingly dependent on fast connectivity and access, with extremely low „entry costs" (Society, 2015).

Cyberspace is linked to a number of related terms, such as virtual reality, online environment, digital space, which together form a conceptual framework that is still malleable. Over time, research has shown that, as the phenomenon has developed in width, depth, and nuances, it has generated a variety of perspectives for analysing definitions and theories in cyberspace. The diversity of notions in the definition of terms is a major obstacle in creating common agreements between states on how to work together on legal issues related to cyberspace. Despite these approaches, we consider it appropriate to define a unified concept based on common issues. Today, cyberspace has become the backbone of what is called the knowledge society, conceived as a different environment, in which the implementation of technological innovations must be carried out together with new legal solutions to regulate the negative impact of ICT use.

SECURITY RISK MANAGEMENT

The technological complexity, the wide range of data/information and the high number of threats and incidents in the security and functionality of distributed systems are factors that need to be considered in the development of information systems. The main purpose of the risk management process for an organization shall be to protect it and to fulfill its mission. In this respect, the risk management process should not be treated as a technical function carried out by experts operating and managing the IT system, but as an essential element in the functioning of an organization. Developing an organization's resource protection strategy is a complex and sensitive process in terms of the components involved in risk management. In literature, risk management is defined as „the process of identifying vulnerabilities and threats within an organization to develop measures to minimize their impact on information resources". In general, most organizations focus on physical protection (especially network infrastructure vulnerabilities, computing systems) and fail to determine the effects on the most important resources.

An incomplete approach leads to a gap between the operational and the total security needs, leaving valuable assets at risk. Current approaches to information security risk management tend to be incomplete as they fail to include all the risk components (and vulnerabilities) in the analysis. Risk management is the process that allows the management level to strike a balance between the operational costs, the financial resources needed to implement protective measures and the achievement of resource protection objectives (infrastructure, computing systems, applications, data) that support the work (Commision, 2018).

According to the NIST, risk management is „the process that allows its managers to balance the operational and financial costs of protection measures to make a gain in relation to the protection capacity of the information systems and data that support the mission of the organization". This definition is based on the possibility that an event (unforeseen or anticipated by the decision makers with a certain probability) will materialize and will adversely affect certain aspects of the operational activity.

Risk management planning is the process by which it is decided how to approach and plan risk management activities. Before initiating any risk management action, the existence of a potential risk for the system under consideration, with regard to the area of activity, shall be assessed. This assessment shall consider all the activities involving the scheme which may contain a potential risk. This provides a list of activities and a classification of potential risks into risk-free, low-risk and high-risk activities (Government, 2018).

The overall risk management process shall consist of the following steps:

- assessment, identification and classification of risks that may affect organizations (planning and collection of risk-related data, risk hierarchy);
- coordination of the decision-making process, the identification and evaluation of control measures considering the cost-benefit ratio (definition of functional requirements, identification of control solutions, review of solutions against requirements, estimation of risk reduction, selection of risk mitigation strategy);
- implementation of control measures to reduce or eliminate risks (search for alternative approaches, organizations for control solutions);
- determining the effectiveness of the control measures and the degree of protection afforded by existing checks (establishment of security risk forms, measurements of the effectiveness of these checks).

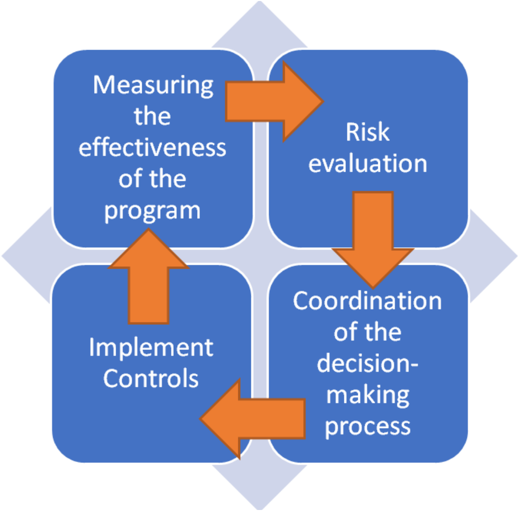
Measuring the effectiveness of the program
Risk evaluation
Coordination of the decision-making process
Implement Controls

Fig. 1:Risk management process (Government, 2018)

Risk analysis (risk identification and assessment) is one of the most important aspects of safety and it in line with good practice in the field. The organizations should address the risk in four steps (Government, 2018):

- identify and assess important information;
- identify and assess threats;
- vulnerability assessment;
- risk assessment.

The risk analysis shall include a process of identifying and classifying security risks, determining the magnitude of risks and identifying areas with high-risk potential. Risk analysis is part of the complex set of measures called risk management. The risk assessment is the result of a risk analysis process.

Risk reduction requires preventative measures to be adopted in case of occurrence of a risk. An organizational set of costs is required for implementation that must be matched with the extent of damage resulting from the exploitation of vulnerabilities so that management factors decide which risks are to be prevented, limited or accepted. The most important approaches used in the risk analysis processes are quantitative, qualitative and cost-benefit analysis.

In essence, risk analysis is a method (qualitative and/or quantitative) used to assess the risk impact on potential decisions in a given situation. The aim of such a move is to guide the decision maker in order to better address decision-making problems marked by a certain degree of uncertainty. The risk quality analysis is a process of assessment which prioritizes risks according to their potential effect on the system (potential loss).

Qualitative analysis is a way of determining the significance of the risks identified and a guide of measures used to respond to them. This approach to risk analysis is the most widespread method, only the value of the potential estimated loss being used. Most methodologies for qualitative risk analysis use a set of interrelated elements (threats, vulnerabilities and controls) which must be proportionate to the vulnerabilities of the system and the likelihood of an undesirable event occurring.

Quantitative risk analysis is the process of assessing in a numerical way the probability and impact of each risk on the fulfilment of the roles of the system and its influence on the overall risk of the system. This risk analysis model shall be based on the determination of the probability of an event occurring and on the estimation of the likely losses (impacts) it would cause. Quantitative analysis makes it possible to rank events in order of risk by calculating the value of an event and multiplying potential losses with the probability of occurrence of that event.

The cost-benefit analysis must be included in the decision-making process as it makes an estimation and comparison of the relative values and the costs associated with each proposed control; it is basically the efficiency criterion used to choose the controls to be implemented. Used as a tool for decision-making, the cost-benefit analysis compares the total costs with the benefits expressed in financial terms. Costs should include the cost of equipment purchase and operating costs (maintenance, user training, supplies, etc.), but also the opportunity costs.

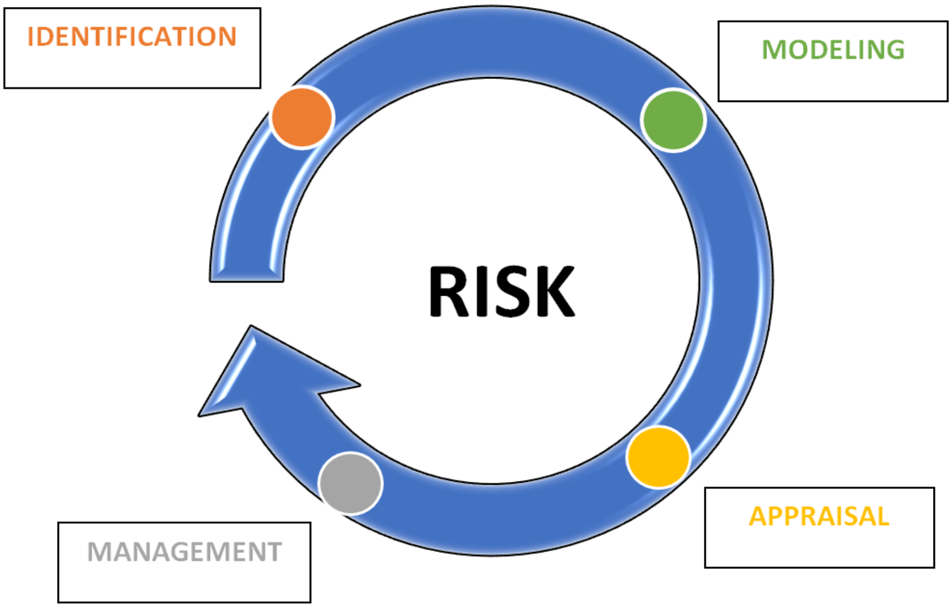

Fig. 2: *The steps of the risk management process*

It is widely accepted by information security experts that risk estimation is part of the risk management process (dealing with estimation, planning, implementation, control and monitoring of the implemented controls) and of the security policies applied.

Security control measures used to protect assets and resources without proper risk assessments may result in an overprotection, making security an obstacle to operational processes, or in an inadequate protection that will expose the organization's key assets and resource to various threats (Society, 2004).

CONCLUSIONS

The continuous regulation of cyberspace at international level is necessary and, at the same time, it is welcome, being an obligation and a duty of the entire international community and requiring the establishment of unitary benchmarks that allow the standardization of the technology used.

This article started from the clarification of the notion of cyberspace by highlighting its characteristics and vulnerabilities, so that a more concrete and complete picture of its complexity could be provided.

Evolutionary trends in the expansion of the number of devices connected to the Internet, the innumerable possibilities of exploiting their vulnerabilities, the ease with which these activities can be performed and the limited possibilities of detecting attackers lead us to the idea that traditional security tools must be supplemented with new elements that would help limit the chances of being subject to a cyber-attack.

International cooperation plays a key role in this area, as cybersecurity challenges the transcending of borders and the extension to the level of globally interconnected systems. Cyber threats and vulnerabilities continue to evolve and intensify, which will require a closer cooperation, especially in the management of large-scale cross-border cybersecurity incidents. Collaboration with European and international entities is absolutely necessary, whether they are educational institutions, research centers, private companies or government institutions.

Operational cooperation and crisis management in cybersecurity should be based on strengthening the existing operational prevention capabilities, in particular by modernizing the pan-European cybersecurity exercises.

From the point of view of the implemented measures, Romania is at an average level, with a series of initiatives taken on both legislative and awareness sides of the field. The current legislative framework needs to be supplemented, so that the attributions of state institutions in the cyber field and the obligations of legal persons for the protection of cyber infrastructures can be clearly established.

Greater transparency of cyber authorities, together with a proper promotion of collaborative initiatives between the private and governmental sectors, can reduce the perception of abuses that can be committed by competent authorities, favoring an advanced understanding of the legislative issues.

In particular, the conclusions of the article aim to increase public awareness of the risks to which they are exposed in an organization, both individually and collectively, by not implementing the minimum-security measures.

REFERENCE LIST

Commision, E. (2018, May 7). European Institute of Romania Seminar „Current challenges in the field of cyber security - impact and contribution of Romania in the field" nia - Current challenges in the field of cyber security - Impact and contribution of Romania. Retrieved from ec.europa.eu: https://ec.europa.eu/romania/events/20180502_seminar_provocari_securitate_cibernetica_impact_romania_ro

Government, G. S. (2018, July). Risk management methodology. Retrieved from sgg.gov.ro: https://sgg.gov.ro/new/wp-content/uploads/2018/07/Metodologia-de-management-al-riscurilor-2018.pdf

Monitor, O. (2010, November 12). EMERGENCY ORDINANCE no. 98 of November 3, 2010. Retrieved from legislatie.just.ro: http://legislatie.just.ro/Public/DetaliiDocument/123547

Monitor, O. (2012, June 18). Law no. 82/2012 on the retention of data generated or processed by providers of public electronic communications networks and providers of electronic communications services intended for the public. Retrieved from www.lege5.ro: https://lege5.ro/Gratuit/gmzdcmrwga/legea-nr-82-2012-privind-retinerea-datelor-generate-sau-prelucrate-de-furnizorii-de-retele-publice-de-comunicatii-electronice-si-de-furnizorii-de-servicii-de-comunicatii-electronice-destinate-publicul

Monitor, O. (2013a, May 23). Decision no. 271/2013 for the approval of the Cyber Security Strategy of Romania and of the Action Plan at national level regarding the implementation of the National Cyber Security System no. 1157/2013 on the approval of the National Security Industry. Retrieved from www.lege5.ro: https://lege5.ro/Gratuit/gm3demzrgq/hotararea-nr-271-2013-pentru-aprobarea-strategiei-de-securitate-cibernetica-a-romaniei-si-a-planului-de-actiune-la-nivel-national-privind-implementarea-sistemului-national-de-securitate-cibernetica

Monitor, O. (2013b, December 13). Decision no. 1157/2013 on the approval of the National Security Industry Strategy. Retrieved from www.lege5.ro: https://lege5.ro/Gratuit/gm4donruha/hotararea-nr-1157-2013-privind-aprobarea-strategiei-industriei-nationale-de-securitate

Monitor, O. (2015, June 23). Decision no. 33/2015 on the approval of the National Strategy for the defense of the country for the period 2015-2019. Retrieved from www.lege5.ro: https://lege5.ro/Gratuit/g4ydqobugm/hotararea-nr-33-2015-privind-aprobarea-strategiei-nationale-de-aparare-a-tarii-pentru-perioada-2015-2019?pid=80097924#p-80097924

Society, M. O. (2004, May). Introductory guide for the application of the legal provisions regarding cybercrime, Bucharest, May 2004. Bucharest, Romania.

Society, T. M. (2015, February). Digital Agenda for Romania 2020. Retrieved from: www.comunicatii.gov.ro: https://www.comunicatii.gov.ro/agenda-digitala-pentru-romania-2020/