CYBERSECURITY AND MACROECONOMIC VULNERABILITIES

Robert Claudiu HELLVIG, Drd
University of Targoviste, Romania

Abstract: *Managing the risks of national information systems is vital in order to ensure an indestructible information security. The risks associated with any type of cyberattack depend on three elements: the threats – who initiates the attack, the vulnerabilities – the sensitive areas on which the attack is focused and the impact – the effects of the attack. The management by the security departments of the risks generated by cyberattacks involves eliminating the threat source, approaching the vulnerabilities by strengthening ICT assets, reducing the impact by mitigating the damage and restoring the functions. The optimal level of risk mitigation depends on the sectors in which a public institution operates.*

Keywords: *security, information, risk, vulnerability, protection*

The actual context definitely imposes the use of the online environment in our daily activities, both at work and at home, as well as the transfer of information between all kinds of entities, from public institutions, organizations and companies to end users. The virtual environment is evolving, which creates new opportunities for the development of the informational society, as well as risks with regards to its functioning.

Information, like every other vital resource of an organization, is an extremely important component for the Romanian public institutions and therefore, it requires an adequate protection. Information has become the target of increasingly numerous and diverse threats and vulnerabilities in both the public and the private environment. Information security systems protect the organizations against a diversified range of threats, in order to ensure the continuity of the activity, the veracity of information, the resilience to cyberattacks and the minimization of information theft risks threatening the institutions from an informational point of view.

In fact, what does the concept of information security represent? Due to the fact that it has a wide applicability and scope, it ensures the integrity, the safety and the availability of information. Of course, the permanent modernization and application of innovation in the IT field also exponentially increases the risk, while allowing at the same time the emergence of new risks, totally unknown to manufacturers up to that moment. Precisely for that reason, the public or the private users must be one step ahead and implement new control methods in a continuous and professional manner. It is extremely easy to give examples of risks in this sector: the emergence of the new capacity portable memories gives to those who want to perform illegal actions the chance to copy unauthorized data or steal it much easier, not to mention the Internet connection as well as networking, which substantially facilitate the data theft.

The technology which has become more and more complex over the years is nowadays present in almost every activity of the modern society, including in government services, whose tendency is total digitization. The latest exponential progress with regards to the processing power and the storage capacity led to the need for rapid, small sized, light, cheap and easier to use IT equipment. The IT industry and communication industry got closer and closer as market demands until they formed a combined, multidisciplinary sector called in the specialized terminology Information and Communication Technology.

The ICT equipment is very complex and highly interdependent, and the dysfunction of one its components can directly affect the functioning of the others. Information technology insiders have expressed their concern over the last few decades about protecting these systems against cyberattacks, which are actions performed by unauthorized individuals in order to illegally access IT systems for the purposes of business interruption, theft, destruction or other illegal actions.

The totality of actions to protect information systems and the data stored within them is called cybersecurity. This broad and insufficiently explained concept, cybersecurity, may be a useful term, but it cannot be identified through a precise definition. It usually refers to one or more of the following aspects:

- the activities and measures intended to protect both computer systems, computer networks, software applications, related hardware/software components and the data/information they store or transmit against attacks, interruptions of their functioning or other threats coming from the cyberspace;
- the situation in which you are protected against such illegal attacks;
- totality of efforts made to implement these activities aimed to mitigate the risk and to improve the quality of services.

In the case of public institutions, cybersecurity is related to the concept of information security. The designation can be explained through the activity of protecting all information and information systems of the state against unauthorized access, against unauthorized use, disclosure, interruption, modification or destruction. Sustained efforts are made to ensure the integrity, the confidentiality and the availability of information.

The governance in the field of cybersecurity shows numerous deficiencies in the public sector of Romania, which affects its ability to deal with cyberattacks and limit them, while undermining the possibility of a coherent approach at the overall level of the public system. That is precisely why the difficulty lies in strengthening cybersecurity governance which can be counteracted by ensuring a climate based on trust which is essential to the process of strengthening the overall cyber resilience. Improving the information exchange and the coordination between the public and the private sectors remains a challenge hard to overcome, which can minimize the effectiveness of the response to cybersecurity incidents.

The digital ensemble has become so complex that it is practically impossible to repel a cyberattack.

The solution to this challenge consists in rapidly detecting and responding to information security incidents. Unfortunately, cybersecurity has not yet been fully integrated into the current Romanian mechanisms of crisis response coordination which limits the national capacity to react to large-scale cross-border cyber incidents.

The protection of infrastructures and vital societal functions is essential. The hypothetical possibility of interfering with electoral mechanisms and intervening in the online and offline disinformation campaigns is a continuous challenge. The current interactions caused by the cyber threats that our country faces require an ongoing commitment and a constant compliance with the primary European values in the field. There is no single, standard, internationally accepted definition of the concept of cybersecurity. This concept integrates all warranties and measures adopted to protect the information systems and their users against the unauthorized access, against attacks and damage in order to preserve the data in its entirety and to protect it.

Cybersecurity encompasses preventing and detecting cyberattacks, responding to them and recovering after an incident. Incidents can be caused intentionally or unintentionally and cover a very wide range of situations, starting from accidental disclosure of information up to attacks on vital infrastructures, the theft of personal data and even interference with democratic processes. All

these incidents can reflect negatively on individuals, public institutions and communities in general.

As for the cybersecurity of hardware and software infrastructures of the Romanian Government, this is the state of normality of information in these systems, of the digital resources or of services offered by the public institutions in the cyberspace (Decision no. 271/2013). This state implies ensuring the following objectives**:**

- **confidentiality –** the property that information, services or resources of information systems are not available to unauthorized persons or processes;
- **integrity –** the property of preserving the accuracy of information, services or resources of information systems;
- **availability** – the property that information, services or resources of information systems are available at any moment to authorized persons or processes;
- **authenticity –** the property of ensuring the identification and authentication of persons, devices and services of information and communication systems;
- **non-repudiation –** the property that the data in the information systems cannot be repudiated (denied, disputed) subsequently.

Being a vast field, security has been divided into fields of division in order to make it easier to manage. The division allows professionals in the field a more precise approach with regards to training, research and labor division. At the level of the International Organization for Standardization (ISO) and of the International Electrotechnical Commission (IEC), which are the international standard-setting confederations in all existing fields, 12 sub-fields of network security have been defined as follows:

- Risk assessment which represents the first step in risk management and determines the quantitative and qualitative value of the risk in connection to a specific situation or a known threat;
- The security policy is the document setting the coercive measures and the behavior of the members of an entity and detailing the means of accessing the data, which data is accessible and to whom;
- Organizing the information security is the model of information security management developed by an organization;
- Asset management represents the inventory of information assets drawn up according to a classified scheme;
- Human resources security defines the security procedures regarding the employment, the posting and the departure of employees from the organization of which they will be, are or have been a part;

– The physical and environmental security describes the protection measures for the data centers within an organization;
– The communication and operations management describes the security measures for networks and information systems;
– Access control refers to restrictions placed on the direct access to the network, systems, applications and data;
– The acquisition, development and maintenance of information systems defines the application of security measures within the applications;
– The management of information security incidents deals with how the system anticipates and responds to security breaches;
– The management of business continuity describes the measures of protection, maintenance and recovery of an entity's vital processes;
– The conformity describes the process of ensuring compliance with information security policies, standards and rules.

All of these fields were created precisely to use as a basis for the development of efficient security standards and practices and to give confidence to activities carried out between organizations.

The cyber threats to public institutions can come from individuals or from other states that may have different interests such as: financial gains, the theft of sensitive or classified information, political and strategic reasons, discrediting, etc.

Thus, cybersecurity becomes a competition between attackers and defenders. The attackers constantly analyze the vulnerabilities of information systems, which can occur in various contexts, and the defenders have the obligation to reduce these vulnerabilities, especially the most important and challenging ones which are those acts committed by persons inside the system (insiders) as well as previously unknown vulnerabilities (zero-day vulnerability). However, there may also be known vulnerabilities, which can be fixed, but which cannot be implemented in most cases due to budgetary or operational constraints.

An undetected cyberattack on a public institution's information system can compromise the confidentiality, the integrity and the availability of data and information it manages. The consequences of such an attack on an institution can be the cyber theft or the cyber espionage, obtaining financial, personal or professional information, often without the knowledge of the victim, slowing down or preventing the access of legitimate users to an information system, taking control over an information system to be used in cyber attacks on other systems, destroying or interrupting industrial control systems that can lead to malfunctions of the equipment they control (generators, pumps, power plants). All these can generate major effects at the regional or state level.

Based on previous experiences, we can say that, in most cases, cyberattacks have a limited impact, while a successful attack on certain components of vital infrastructures of a public institution could have significant effects on national security, national economy and the safety of citizens. Reducing these risks at state level involves removing known threat sources as well as mitigating vulnerabilities and their impact.

Vulnerability is a weakness of a hardware or software system which allows unauthorized users to gain access to it (Mihai & Petrică, 2014). The vulnerabilities of information systems are usually found in the hardware infrastructure, in software solutions or the human component. The information systems are first of all vulnerable to classic attacks when a user manages to physically enter the premises of computer systems and steal confidential information. To prevent this from happening, public institutions must take measures to ensure the physical security of ICT equipment by placing it in secure areas, restricted to unauthorized persons. The security in such areas is done by restricting the access, which can take place via human security, the use of intercoms, access cards or biometric data scanning devices that authenticate users who have an entry permit.

Another kind of vulnerability of information systems is represented by the natural disasters (earthquakes, floods, fires) or by accidents (for example voltage drops or power surges), which can cause the physical destruction of computer equipment. That is why great care must be taken in placing the equipment in adequate, secure spaces in order to mitigate the risk of natural threats.

The most serious threats with regards to consequences are those allowing hackers the accesss to the most sensitive data and information of the information system. These attacks start by infecting computer systems with trojan viruses or computer worms that can penetrate the security of the information system and thus, an unauthorized user can connect to the system. These are considered extremely serious vulnerabilities because they allow the total access of unauthorized users to the operating system and to the database of the system, having the capacity to steal or even delete important or confidential government data.

A separate kind is represented by zero-day vulnerabilities, unknown to software developers and providers and which can be exploited by cybercriminals, without there being a known fix for the security breach, or the attack committed.

The causes for the emergence of vulnerabilities or security breaches in an information system can be multiple and here are some of them in what follows:

– programming errors of operating systems or of computer applications;

– improper configuration of operating systems or applications;

– the level of knowledge in the field of system of network administrators;

– lack of support from software developpers in fixing possible application crashes.

Still, we must admit that one of the greatest vulnerabilities of an information system is the available human resource dealing with the configuration and the managemnt of information systems. As a result of insufficient practical experience or of an incomplete documentation regarding certain configurations of the operating system or other installed applications, cybersecurity can be totally compromised.

Any information system has vulnerabilities. We cannot strongly state that there is a is 100% safe system. Such vulnerabilities are used in many attacks targeting an information system directly, and we can give the example of malware attacks, or indirectly, in the case of the information system involved in a DDoS attack.

Cyberattacks have been taking a particularly large scale recently, some of them can be catalogued as global epidemics precisely because of the high spreading speed in the virtual environment. The threats specific to information systems have as common elements a very strong dynamic and a global character, traits which exponentially increase the degree of difficulty in ther identification and, implicitly, their removal.

Cybersecurity is a vital component in the actual context of national security, it is highlighted by the multitude of development directions in the field. The modernism, the technological explosion and the automation of most activity areas of a society determine the field of cybersecurity to be a priority in the development of national defense strategies at state level.

At this point, Romania is in the midst of activities designed to strenghten the national cybersecurity, from a legislative, institutional and procedural point of view. Therefore, significant efforts are being made at the level of authorities in the field. According to the reports of these institutions, Romania is not only a country that generates cybersecurity incidents or playing a transitory role for external attackers, but it is also turning into a favourite target of cyberattacks such as APT, DDoS or ransomware.

The extent to which the the current legislative regulations become operational at the level of public institutions in Romania is unfortunately quite low. This fails to provide the necessary prerequisites for preventing and counteracting with maximum efficiency cyberattacks with a higher degree of complexity. These realities must make us aware of the fact that we have a major responsibility in strengthening the institutions which have attributions

in the field of cybersecurity. This must be a top priority, precisely in order to ensure the premises of a rapid reaction to cyber incidents.

The international cooperation has a decisive role in counteracting this phenomenon because cyberattacks go beyong state borders, reaching the level of globally inteconnected systems. Cyber threats are constantly evolving and intensifying at an accelerated pace. A much closer cooperation in managing cross-border cybersecurity incidents is urgently required. The collaboration with transnational entities is absolutely necessary, be it government institutions, research centers or higher education institutions.

The adoption of a comprehensive legislation in the field of cybersecurity supporting the development of the national defense capacities is an actual, acute and necessary priority. Ensuring a safe cyberspace must be the responsibility of the competent authorities in the field. But we should not forget that the responsibility belongs not only to the state, through its institutions. Each of us is an integral part of the notion of state. Therefore, the responsibility must equally belong to the private sector and to the civil society. In order to develop the culture of cybersecurity, we believe that the most important mechanisms are education and research, the public-private partnerships as well as the international cooperation mechanisms.

References

Brooks, C., Craig, P., & Short Somerset, D. (2018). *Cybersecurity essentials*. John Wiley & Sons.

Decision no. 271/2013 for the approval of the Cyber Security Strategy of Romania and the National Action Plan regarding the implementation of the National Cyber Security System, Government of Romania, Official Gazette, no. 296 of May 23, 2013.

Mihai, C., & Petrică, G. (2014). *Information security.* Second edition. Craiova: Sitech Publishing House.

Sammons, J., & Cross, M. (2017). *The basics of cyber safety*. Amsterdam, Elsevier.