Adrian-Viorel DRAGOMIR
Doctoral School Industrial Engineering and Robotics, Politehnica University of Bucharest
Constantin-Adrian BLANARU
Permanent Electoral Authority

THEORETICAL ASPECTS REGARDING CYBER SECURITY IN ROMANIAN PUBLIC INSTITUTIONS

Keywords
Cyber-security;
Strategy;
Implementation;
Cyber-treats;
Information technology;
Resilience;

Abstract

Technology has become more complex as the years have passed, being present in almost every activity of modern society, including government institutions, where the trend is the digitization of processes, especially those representing services to the population. Recent technological progress has increased exponentially in terms of processing power and memory capacity, and the world has started to need mobility, which has led to the need for fast, small-scale, light-weight, cheap and easier-to-use ICT equipment. The IT industry and the communications industry have become increasingly close to market requirements until they have formed a combined, multidisciplinary sector called Information and Communication Technology in specialized terminology. Technology opens up new opportunities, with new products and services that can be an integral part of the activities of public institutions, to meet the urgent need for digitalization in this field. With the digitization process, the risk of being a victim of a form of cybercrime increases exponentially, and the social and economic impact of these phenomena is becoming increasingly important. Thus, most states have focused their efforts on strengthening cybersecurity and digital autonomy in these critical times, Romania being one of them.

In the context of changes of the society, global communications, affordable and high-speed connections available to all categories of users, taking place today and taking into account the unprecedented development of software programs and applications, information security has become a very important task for all governments in the European Union[i].

The managerial decision-making that is fit for these times requires access to large amounts of information and a distributed way of working as the place of deployment and as delegation of powers. The need to use data networks requires security and protection of the information that flows through their intermediations, thus becoming basic requirements for any digital system, application or service.

The transmission of data using the Internet network can result in the transit of multiple communications networks and thus enable users on the networks through which the data is transited, to intercept and/or modify it. Similarly, through unauthorized access to system resources, users on the same network as the transmitter and receiver can modify or destroy data and information.

The need for security is based on the fact that IT systems cannot be 100% secure, with the only way to ensure security being to develop and implement security solutions that make it difficult to compromise the system. For public institutions, ensuring a secure environment through the use of information systems is operationally binding requirements of today's society, effectively becoming an intensive and continuous concern for possible cyber risks and threats[ii].

Ensuring security of information is represented by the development of rules, protection policies, action plans for activities aimed at compromising information and data. Cybersecurity is becoming a complex area that requires multi-level engagement of mechanisms that can be addressed in public policies at the level of the administration.

Today`s ICT equipment is complex and interdependent, and the failure of one of them can affect the operation of others. Industry experts have recently expressed concerns about protecting these systems from cyber-attacks, which are actions by unauthorized persons to access IT systems for the purposes of downtime, theft, destruction or other illegal actions.

The Romanian legislative framework regarding cyber security is incomplete, the existing gaps in Romanian legislation, as well as the inconsistent transposition of the European acquis into legislation can hinder the digitization process or lead to chaotic implementations of new technologies.

Without a consistent and harmonized legislative framework, aligning investment levels with objectives is difficult, this means not only increasing investments in cybersecurity, investments that are very low and fragmented in Romania, but also increasing the impact of these investments. These dysfunctions can be remedied by better exploiting the results of research spending, as well as by ensuring the effective targeting of cybersecurity budgets to institutions with responsibilities in this area and by funding them in a way that transforms into effective and sustainable entities.

Creating a clear overview of Romania's cybersecurity spending is essential to enable government decision-makers to know the areas suffering from underfunding in this area and to eliminate them in order to achieve their stated objectives. As there is no budget specifically earmarked for funding the cybersecurity strategy, it is not very clear what money is being spent and for what purpose[iii].

In a context where political decision-makers set cybersecurity as priorities for good governance, budgetary constraints in providing adequate technical or human resources for public institutions with cyber responsibilities can hinder the achievement of these priorities of our country. Addressing these difficulties requires, on the one hand, finding alternative financing solutions, such as European funds or grants made available by other countries or funding institutions, in order to implement cyber security solutions and on the other hand to find ways to attract and preserve talented human resources in the country, because for financial reasons they are tempted to leave Romania for higher wages or better working conditions.

As the global scarcity of human resources in cyber security is increasing, skills development and employee awareness are key issues both in public institutions and at all levels of society. Currently, there are only a few standards in the Romanian labor market in the areas of training, security solution specific certification or cyber risk assessment.

The risk management of state information systems is considered fundamental to ensuring effective IT security. The risks associated with any attack depend on three factors: Threats (who attacks), vulnerabilities (the weaknesses they attack) and impact (what does the attack). Managing cyber-attacks risks by security departments involves removing the source of the threat, addressing vulnerabilities by strengthening ICT assets, mitigating impact by mitigating damage and restoring functions. The optimal level of risk reduction will vary depending on the sectors in which a public institution operates.

Cybersecurity management has numerous shortcomings in the Romanian public sector, limiting its ability to cope with attacks or limit its impact. These deficiencies may undermine the possibility of a coherent approach to security across

the public system as a whole. The challenge is therefore to strengthen cyber security management that can be tackled by providing a trusted climate that is crucial to enhancing cyber resilience.
Improving information sharing and defense coordination against attacks between the public and private sectors remains a difficult challenge to overcome, with a lack of such activities likely to reduce the effectiveness of responding to cyber security incidents.
ICT systems have become complex, with multiple variants or brands of appliances and software, this makes it almost impossible to prevent every attack. The response to this challenge is to detect and respond rapidly to cyber security incidents.
Cybersecurity is not yet fully integrated into the crisis response coordination mechanisms implemented in Romania, which may limit the country's security capabilities to respond to large-scale cross-border or hybrid cyber incidents.
The protection of critical infrastructures and societal functions is essential. The possible interference of malicious persons or entities in state information systems that can steal, exchange or compromise data or information from these systems and disinformation campaigns is a major challenge for today's security. The current challenges posed by the cyber threats facing our country require continued commitment and a firm and constant respect for the fundamental values of the European Union in this area.
Cyber threats to public institutions can come from individuals or other countries that may have different interests, such as: Financial gains, theft of sensitive or classified information, political and strategic, discrediting, etc.
We have not identified a standard and universally accepted definition of cyber security in the research of bibliographic resources dedicated to this area. This concept should cover all measures necessary to protect the information systems and their users against unauthorized access, attacks and related harm, in order to ensure the confidentiality, integrity and availability of their data.
Measures to protect the information systems and data that are stored within them are called, in unanimously accepted terms, security of confidentiality. This concept refers to one or more of the following:
• activities and measures designed to protect both computer systems, computer networks, software applications and the data or information contained therein;
• the condition or quality of being protected against the transmission of computer viruses, disruption of operation or other cyber-space threats;
• the wide scope of efforts to implement and improve the above-mentioned activities.
Cybersecurity involves preventing or detecting cyber incidents, responding to them and recovering from them. Incidents are usually intentional and cover very diverse situations, such as accidental disclosures, attacks on critical infrastructures, personal data theft and even interference in democratic processes. All these impacts can have far-reaching negative effects on individuals, public institutions and communities in terms of their image or credibility.
The concept of cybersecurity should not be limited to the security of information systems and communications networks, but should cover any illegal activity involving the use of technology. Therefore, this concept covers all types of cybercrime, such as, launching attacks with computer viruses, fraud with cash-free means of payment, online dissemination of materials containing misinformation or false news, unauthorized denial of services, phishing, etc., and can cover both systems and content. Cybersecurity can also cover disinformation campaigns aimed at influencing internet public debates and suspected interference in elections.
Cybersecurity can be described as a competition between attackers and defenders. Attackers constantly analyze the vulnerabilities of information systems that may arise in different contexts, and defenders are obliged to reduce them, especially the most important and challenging acts produced by persons inside the system and previously unknown vulnerabilities (zero-day vulnerability). However, there may also be known vulnerabilities, with methods of resolution, but which in most cases cannot be implemented due to budgetary or operational constraints.
As for the cyber security of the Romanian state's hardware and software infrastructures, this is the state of normality of information in these systems, digital resources or services provided by public institutions in the virtual environment. The state of normality of the data and information managed through the information systems whose owner is the Romanian state implies the following objectives[iv]:

- confidentiality - the property that information, services or resources of information systems are not available to unauthorized persons or processes;
- integrity - property to maintain the accuracy of information, services or resources of information systems;
- availability - the property that information, services or resources of information systems be accessible at any time to authorized persons or processes;
- authenticity - property to ensure the identification and authentication of persons, devices and services having access to information and communication systems;
- non-repudiation - the property that data in computer systems cannot be denied or challenged at a later date.

Because it covers many technical aspects, cybersecurity has been separated into several divisions to make it easier to manage. This division enables professionals in this field to address training, research and division of labor more accurately. At the level of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), which are the international regulatory confederations in all existing areas under ISO/IEC 27000/2018[v], 12 network security sub-domains have been defined as follows:

- The risk assessment which represents the first step in their management and determines the quantitative and qualitative value of the risk related to a specific situation or known notification;
- Security Policy is the document that sets out enforcement measures and behavior of members of an entity and details how to access data, what data is accessible and to whom;
- Information security organization is the information security management model developed by an organization;
- Asset management means the inventory of information goods drawn up in accordance with a classified scheme;
- Human resources security defines security procedures regarding the employment, secondment and departure of an employee of the organization from which he or she will be, or has been a Member;
- Physical and environmental security describes protection measures for data centers within an organization;
- Management of communications and operations describes the security measures for networks and information systems;
- Access control relates to restrictions on direct access to the network, systems, applications and data;
- Acquisition, development and preservation of information systems defines the application of security measures within applications;
- Information security incident management treats how the system anticipates and responds to security breaches;
- Business continuity Management describes measures to protect, maintain and recover processes and systems that are critical to an entity;
- Compliance describes the process of ensuring compliance with generally accepted information security policies, standards and rules.

The risk management of state information systems is considered fundamental to ensuring effective IT security. The risks associated with any attack depend on three factors: threats (who attacks), vulnerabilities (the weaknesses they attack) and impact (what does the attack). Managing cyber-attacks risks by security departments involves removing the source of the threat, addressing vulnerabilities by strengthening ICT assets, mitigating impact by mitigating damage and restoring functions. The optimal level of risk reduction will vary depending on the sectors in which a public institution operates.

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

These sub-areas have been created to serve as a common basis for the development of effective security standards and practices and to give confidence in the exchange of data and information between organizations. On the same criteria of efficiency and ease of learning, cyber-attacks on data networks have also been divided, namely: recognition, access and the impossibility to meet a legitimate request.

Cybersecurity can be achieved through proactive and reactive security measures including security policies, standards and models, risk management and ICT systems protection solutions.

Legislative initiatives of the Romanian Government or cybersecurity institutions are designed to address a number of short- and medium-term needs in the field of cyber security, namely: disaster prevention, prevention of cyber spies, reduction of the impact of successful attacks, improved collaboration within the private cybersecurity sector, clarification of the roles and responsibilities of institutions responsible for preventing and combating cybercrime. These needs have arisen in the context regarding the challenges of design, economic stimulus, consensus and the environment.

In our country, cybercrime is manifested through cyber attacks that aim to compromise different state networks and information systems through multiple ways and tools: Malware, ransomware, DDoS attacks, defacement, fictitious asset auction fraud, compromise of user's accounts on e-commerce sites, phishing sites for bank data collection, credit card fraud, compromise of ATMs and extract confidential information from customer cards.

Cyber attackers use social engineering to persuade state service officials to take action to infect the information systems they use or manage and to disclose sensitive or confidential information, and through such actions attackers gain access to the computers under attack, and after this these PC`s becomes part of botnet networks, which are then used to carry out other coordinated cyber-attacks, usually DDoS, against other infrastructures.

At the level of cyber security institutions, there is a worrying trend in the involvement of early and even minor individuals in cyber-crime, who are not aware of the legal consequences of such actions. This is why the general public needs to be better informed

by means of school-based campaigns on combating and preventing cybercrime among children and young people.

The methods for responding to cyber security incidents at the level of our country have been set out in the Romanian Cyber Security Strategy, which was approved by Government Decision No. 271/2013 for the approval of Romania's Cyber Security Strategy and the National action plan on the implementation of the national cyber security system[vi].

Thus, it has been established that cyber security at the level of our country should be ensured through the National Cybersecurity System (SNSC), which is the general framework for cooperation that brings together public authorities and institutions with responsibilities and capabilities in this area, to coordinate national actions to ensure cyber security, including through cooperation with academic medium and business, professional associations and non-governmental organizations. This system functions as a unified mechanism for inter-institutional networking and cooperation aimed at the unified adoption and application of decisions in case of cyber attacks.

The coordination of the SNSC is ensured by the Cyber Security Operative Council (COSC), which is made up of representatives of the Ministry of National Defense, the Ministry of Internal Affairs, the Ministry of Foreign Affairs, the Ministry of Research, Innovation and Digitization, the Romanian Intelligence Service, the Special Telecommunications Service, the Foreign Intelligence Service, the Protection and Guard Service, The Office of the National Register of State Classified Information and the Supreme Council of National Defense.

In addition to the institutions represented in the Cybersecurity Task Council, there are also specialized cybersecurity incident response structures of the type CERT/CSIRT, which include:

• CERT-RO – National Cybersecurity Incident Response Center, national CERT acting as coordinator of the Romanian CERT community;

• CYBERINT - National Cybersecurity Center, national authority in the field of cyber-intelligence, subordinated to the Romanian Intelligence Service which acts to know, prevent and counter the vulnerabilities, risks and threats to the cyber security of Romania;

• CERTMI-CTP – National Technical Response Center for Cyber Security Incidents, Military CERT, of the Ministry of National Defense, with capabilities and responsibilities in cyber defense;

• CORIS-STS - the STS operations Center for Security incident response is the CERT-type entity designated to prevent and respond to security incidents affecting the functioning of the information and communication systems of the Special Telecommunications Service and its beneficiaries;

• RoCSIRT – Academic CERTs, dedicated to the protection of institutions connected to the RoEduNet network;

• CERT-INT – CERTs-type structure of the Ministry of Internal Affairs

An important aspect in this regard is early detection of incidents. Detection tools help to reject most attacks every day. However, digital systems have become so complex that it is impossible to prevent every attack. The sophistication of attacks often means that they remain undetected for long periods of time. Experts therefore say the focus should be on rapid detection and defense.

The development of an effective response to cyber-attacks is crucial to stop them as early as possible. It is of particular importance that the institutions responsible for providing cyber security of the Romanian state and each individual public institution be able to react quickly and in a coordinated manner[vii].

An effective response to cyber attacks means not only limiting the damage but also giving responsibility for these attacks, which is also essential. Tracing and identifying authors, especially in the case of a hybrid attack, can be very difficult due to the increasing misuse of anonymization tools, cryptomonad and encryption. This is the so-called "issue of awarding". Solving this problem is not only a technical issue, it is also a challenge from a criminal justice perspective.

Notes

[i] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, Official Journal EU, 19 July 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L1148, website consulted on 23.04.2021
[ii] Cybercrime To Cost The World $10.5 Trillion Annually By 2025, https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/, website consulted on 23.03.2021
[iii] I.C. Mihai, G. Petrică, C. Ciuchi "Current challenges in the field of cybersecurity –the impact and Romania's contribution to the field, European Institute of Romania, 2018, pp.25.
[iv] Law No 362/2018 on ensuring a high common level of security for network and information systems, Official Gazette No 21 of 9 January 2019, https://lege5.ro/App/Document/gmytiobyga2a/legea-nr-362-2018-privind-asigurarea-unui-nivel-comun-ridicat-de-securitate-a-retelelor-si-sistemelor-informatice, website consulted on 23.04.2021
[v] ISO/IEC 27000:2018 Information technology - Security techniques - Information security management systems, https://www.iso.org/isoiec-27001-information-security.html, website consulted on 27.04.2021
[vi] Strategia de securitate cibernetica a României (Romania's cyber security strategy), https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/StrategiaDeSecuritateCiberneticaARomaniei.pdf/view, website consulted on 24.04.2021
[vii] https://cert.ro/citeste/divulgarea-coordonat-a-vulnerabilit-ilor-component-esen-ial-a-securit-ii-cibernetice, website consulted on 27.03.2021