HOLISTICA Vol 11, Issue 2, 2020, pp.74-84 DOI:10.2478/hjbpa-2020-0020

RISKS AND VULNERABILITIES IN DIGITAL PUBLIC SERVICES. THREAT OF CYBERTERRORISM VS ROMANIA'S CYBERSECURITY STRATEGY

Mihai CONSTANTIN[1]*
Andra-Nicoleta BORȚEA[2]
Denisa-Atena COSTOVICI (MEMA)[3]

Received: February 2020 | Accepted: June 2020 | Published: August 2020
Please cite this paper as: Constantin, M. et al. (2020) Risks and Vulnerabilities in Digital Public Services. Threat of Cyberterrorism Vs Romania's Cybersecurity Strategy, *Holistica Journal of Business and Public Administration*, vol. 11, iss. 2, pp. 74-84

Abstract

The digitization of the administration and the governance process implies a number of advantages that we cannot ignore, but these advantages are supported by a series of disadvantages and unforeseen situations, but by far the biggest threat is Cyberterrorism.

Romania aims both to encourage the indigenous information environment and the services specific to the information society, but also to ensure the fulfilment of the objectives assumed in the area of national security and to protect the fundamental rights and freedoms of citizens.

Currently anyone can be the target of a cyber-attack, and the most important state institutions are usually the first ones targeted. The weak point remains the human factor, the user of the computer system. That is why in any strategy of "Cybersecurity" its awareness and training from the point of view of computer security plays a vital role.

The fact that so far, no attacks have been reported with major impact on public institutions, strategic companies with state and / or private capital or critical infrastructure elements, denotes that the strategy adopted by Romania is a viable one, but must be constantly updated in depending on the dynamics of the threats.

Keywords: Management; Cybersecurity; Cyberterrorism; SRI; CYBERINT

1. Introduction

In the context of the continuous development of the informational society, the IT/communications technology has experienced new valences, significantly impacting the social context and generating mutations in the philosophy of the economic, political and

[1] Valahia University of Targoviste, Doctoral School, Romania, constantintgv@gmail.com
[2] Valahia University of Targoviste, Doctoral School, Romania, andrabortea@gmail.com
[3] Valahia University of Targoviste, Doctoral School, Romania, denisa21co@gmail.com
* Corresponding author

cultural environment with immediate repercussions in the daily life of the modern European citizen (French Government, 2020).

Like conventional crime, cybercrime is polymorphic, it can be achieved without a predictability of time or space. Cyber attackers use a "modus operandi" that varies depending on their abilities and the goals they pursue (The General Directorate of Security and Prevention of the Federal Interior Public Service, Belgium, 2020).

The abrupt increase in the implementation of IT solutions in almost all parts of society has as a direct consequence in changing daily life in all its aspects. Functional aspects of economic, cultural and even political areas have acquired a new dimension in the information age. A dimension without geographical limitations, with a variable degree of anonymity that also generates opportunities, risks and vulnerabilities (at individual, institutional and even state level). The higher the degree of technological development of the company, the more vulnerable it is, and is becoming more difficult to implement IT security solutions.

At the individual access level, security can be ensured by good preventive behaviour of the user. Regarding the institutional or state level, it is necessary to implement policies and strategies in the field of Cybersecurity, in order to ensure the security standards.

Romania aims both to encourage the indigenous information environment and the services specific to the information society, but also to ensure the fulfilment of the objectives assumed in the area of national security and to protect the fundamental rights and freedoms of citizens.

2. State of the arts

2.1. Romanian Intelligence Service, national authority in the field of "CYBERINT"

In the context of amplifying the threats to the national security carried out in cyber space in 2008, the Supreme Council of the Country`s Defense decided that the responsibility of managing the domain "Cyberint" should be assigned to the Romanian Intelligence Service, as the national authority in the field (Romanian Intelligence Service).

With the assignment of this attribution to the Romanian Intelligence Service, the institution has developed its own capabilities, through the “National Cyberint Center” (NCC) meant to provide an adequate response to the new type of threat (Romanian Intelligence Service).

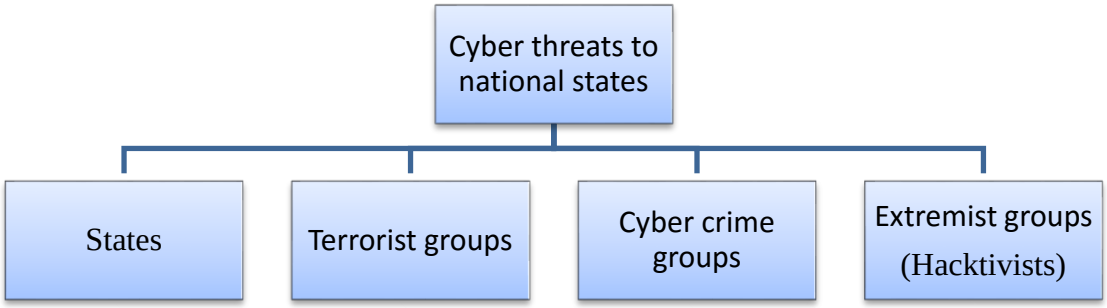
It is important to note that there are several Romanian institutions with concerns in the field of “Cybersecurity” that have niche infrastructures to ensure their own objectives. The most important are those held by the Ministry of National Defense, the Special

Telecommunications Service and the Ministry of Communications and Information Society, through the "National Center for Cyber Security Incident Response"[4].

The National Cyberint Center is designed to act for "knowing, preventing and countering vulnerabilities, risks and threats to cyber security of Romania" (to analyze the cyber-attacks reported in the area of competence and at the same time, to confer the necessary security to the critical IT&C infrastructures) (Romanian Intelligence Service).

The most important forms of cyber threats to the national security of Romania can be classified according to the category of cyber attackers in the following categories: states, cybercrime groups, extremist groups (hacktivists[5]) and terrorist groups.

Figure 1 Categories of cyber attackers



Source: Own creation of authors

The main vulnerability exploited by cyber attackers, whether it is a personal workstation, a computer system belonging to a public institution or an element of critical infrastructure, is the human factor. In this context, it is important to strengthen the security culture of the population, in order to reduce their vulnerability by raising awareness of the risks coming from the virtual space (Cyber Security Guide, Romanian Intelligence Service, p. 5).

The National Cyberint Center periodically develops and implements “awareness” campaigns aimed at potential targets of cyber-attacks (Cyberint National Center, 2018).

2.1.1. Stages of a cyber attack

The level of threats from the virtual area is directly proportional to the accelerated interference of the cybernetic environment in the everyday life. This aspect is statistically confirmed by the number of attacks identified (according to cert.ro annual reports) but also by a perpetual increase in the complexity of cyber incidents. Although each attack

[4]Established by DECISION no. 584 of August 8, 2019

[5] A brief explanation for the term, according to Denning, D. E. (2001), refers to the fact that activism is the merging of hacking and activism, in operations that use hacking techniques.

has its own patent, security specialists emphasize the following conceptual stages of a computer attack (Sînpetru, 2020):

a) "Reconnaissance" data and information collection - This is the initial stage in which we try to obtain as much data from the online environment as a possible target or a victim. The data is collected and analysed to identify a possible vulnerability that will be exploited in the attack. It is mainly aimed at obtaining target data, such as the technologies and IT&C infrastructure used, domains, IP addresses, e-mail addresses and personal data in order to personalize the cyber-attack. As a way, is used an attack of reduced complexity or the accounts of the victim's social networks are exploited.

b) "Weaponization" - Based on the data obtained previously, after the security niche has been identified, the attackers develop the optimal "malware" application.

c) "Delivery" - Step 3 is the actual transmission of the illegitimate application (the "spear-phishing" technique is used, that is, sending to the target of personalized messages according to the data obtained in the initial stage).

With the infection of the target IT&C system and establishing a connection to it via a C&C server (command and control), the attacker achieves its intended purpose, which, depending on the situation, may be the unavailability of the system, theft of money or the extraction of some information.

In some cases, cyber attackers collect information to gain access to data with strategic valence.

2.1.2. Cyber terrorism

The level of security of the systems in public institutions differs in relation to the type of institution, the level of technology / staff training and the investments that they have made on the Cybersecurity component (Essomba, 2017).

Below we present the main vulnerabilities that have been exploited in attacking some European public institutions (most of which are also found in some public institutions in Romania[6]) (European Union Agency for Cybersecurity, 2019, pp. 15-37)

- the non-existence of an internal policy of managing the access accounts - in a digital public institution the differentiation of the users' accounts must be realized so that, each one has access only to the facilities that he / she necessarily needs to carry out his / her tasks. Thus, is observed the need to implement access policies, restrictions, differentiated accounts;

[6] Romanian National Computer Security Incident Response Team - CERT-RO, Threats evolution in Romanian cyberspace, 2018 and Romanian National Computer Security Incident Response Team - CERT-RO, Threats evolution in Romanian cyberspace, 2017, available at: https: // cert.ro/doc/ghid, accessed on 14.04.2020.

- the possibility of using their own equipment at work - is a specific vulnerability for small institutions, which have made a minimal investment in IT equipment, the employee being willing to use his own equipment to achieve professional goals;

- differentiated management of the connection to the internet environment for the different workstations in the institutions - it is important that the workstations are connected to the internet only if the connection is useful in carrying out specific tasks, otherwise it is a major vulnerability;

- the absence of antivirus solutions or the existence of free unpublished variants - the insufficient budgeting of the IT domain has led, in some cases, to the use of antivirus solutions and even illegitimate operating systems that do not provide protection at an appropriate level;

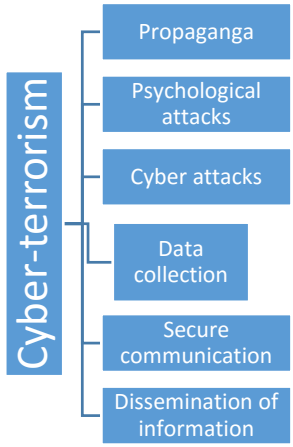
- the loss of specialized human resource (Badea-Mihalcea, 2019, p. 144) at the expense of the private domain - there is a phenomenon of migration of IT specialists from public institutions to large corporations, where the salary obtained is significantly higher and more attractive.

2.1.3. The main cyber vulnerabilities in public institutions

Cyber-terrorism is the convergence of cyber-space and terrorism, with reference to attacks and threats with the attack on computers, networks and stored information, in order to intimidate or constrain a government or population in promoting political or social objectives (Moldovan, 2016).

The notion of "cyber-terrorism" refers to the use of methods specific to the computer war by a terrorist organization. The computer terrorist will concentrate his criminal activity exclusively in the virtual environment, but the expected effect is also felt in the real environment, the result of the attack aiming at significant economic losses, violent actions against people or property, even the death of some people (Sînpetru & Pisargiac, 2019, p. 188).

Figure 2 Dimensions of Cyber-terrorism after Moldovan (2016)



Source: Own creation of authors

Cyber-terrorism takes place in the following dimensions (Moldovan, 2016):

Propaganda

The Internet represents an ideal propaganda platform for terrorist organizations. In the case of Islamist terrorism, propaganda sources mainly use religious arguments to justify political objectives. The propaganda materials are disseminated online, through official channels (websites, electronic publications) or unofficial (groups, forums, blogs), following (Moldovan, 2016):

- exposing the ideology, justifying the cause and popularizing the organization;
- attracting and retaining followers, radicalizing them and recruiting new members;
- fundraising;
- mobilizing followers;

Secure communication

Securing the communications of its members and followers is very important for terrorist organizations, and the Internet offers extensive possibilities in this direction. Operational communications are anonymized and encrypted, using the latest technologies from terrorists (Trivilini, 2016, p. 26). At the same time, we are witnessing an explosion of accessible commercial applications, which makes possible the encrypted communication between users, on condition of anonymity. There have been recent situations, in which members of terrorist cells have used communications systems for electronic games (Moldovan, 2016).

Data collection

Terrorist organizations with international ambitions use the Internet to gather information about the target states. These are studied in a holistic approach, with the aim of identifying vulnerabilities that could be speculated on, including by committing terrorist attacks. Information is collected on potential targets, such as critical infrastructures, public transport, nuclear power plants, accumulation dams, institutions, tourist or diplomatic objectives, public events, personalities' agendas, military bases, airports, ports, stations, headquarters of publications, how the authorities react in case of terrorist attacks, etc. (intelligence.sri.ro, d). Terrorists also use socialization platforms to get in direct contact with the citizens of the target states, from which they obtain data on the social, political, military, cultural developments at the target state level, easy ways to access the territory of the respective state, the degree of alertness of the authorities, the security of certain objectives, etc. (Trivilini, 2016, p. 26).

Dissemination of methodological information

The Internet is used by terrorists including for the dissemination of methodological information, regarding the making of improvised explosive devices or handcrafted weapons, the methods by which online communications can be secreted, the tactics to be adopted to deceive the vigilance of the authorities, updates on the targets targeted by

organizations. Eloquent in this regard are the magazines published regularly in the online environment by Al-Qaeda ("Inspire" magazine) and DAESH ("Dabiq" magazine). The information contained in these publications makes it possible to make "self-directed" improvised explosive devices, which are frequently used in terrorist attacks (Moldovan, 2016).

Cyber-attacks

The online environment offers, in certain circumstances, the possibility of launching cyber-attacks with terrorist motivation, which can target government institutions, the financial-banking system, media trusts, telecommunications companies, energy infrastructures, nuclear targets, etc. (Birta, 2017).

The use of the Internet by terrorist organizations for the purpose of launching attacks on critical infrastructures or strategic objectives is an increasingly popular hypothesis. In recent years, logistically and financially developed terrorist groups have created their own cyber-jihadist structures ("Qaedet al-Jihad al-Electroniyya", set up by Al-Qaeda in 2015 / "United Cyber Caliphate", set up by DAESH in 2014) and began to acquire advanced technologies, respectively to recruit members specialized in hacking activities (Birta, 2017).

Psychological attacks

Terrorist organizations use the Internet to frequently issue threats and publish multimedia material (audio/video recordings, photos) with a strong emotional impact (beheadings, mass executions), meant to induce feelings of fear and insecurity. These online campaigns can be assimilated to psychological attacks with terrorist motivation and target the citizens of the states with which the organization is in conflict. The purpose is to influence the collective mind (lowering the population's trust in authorities, producing social imbalances, breaking out internal conflicts on political, religious, ethnic criteria, etc.)

5. Results

Cyber security strategy of Romania

There are very high expectations, both in the area of protection against cyber acts and in the area of guaranteeing individual freedoms. This balance is difficult because a correct regulation is necessary and the adoption of balanced measures.

Their impact on the common user is considerable (economic crimes, identity theft, etc.), but when the attack is aimed at a state or critical element of the economy (theft of classified information, acts of sabotage), the effects can be disastrous, affecting national security of the state (National Agency for Informational Security Systems)

In response to possible cyber-attacks, European states have developed "Cybersecurity" strategies and created specialized mechanisms for monitoring the virtual environment, they implemented security measures to increase the level of protection in the possible

target areas for attacks and tried to harmonize the legislative framework with the new challenges (Gaftea, 2019, p. 15)

In 2013, in the context of invigorating the challenges of the local virtual environment, through Decision no. 271 The Government of Romania approved the "Cyber security strategy of Romania" and "The national action plan regarding the implementation of the national Cyber security system".

Through the "Cyber security strategy of Romania" the authorities with attributes in the field of "Cybersecurity" are responsible for maintaining a "secure virtual environment, with a high degree of resilience and trust, based on national cyber infrastructures, which will be an important support for national security and good governance, for maximizing the benefits of the citizens, the business environment and the Romanian society as a whole ” (Decision no. 271/2013, section I, point 2).

In addition, the main directions of action are presented in order to ensure the state of normality in the cybernetic environment as the following (Decision no. 271/2013, section II):

-Establishing the conceptual, organizational and action framework necessary to ensure cyber security;

-Development of national risk management capabilities in the field of security;

-Promoting and strengthening the cyber security culture;

-Development of international cooperation in the field of cyber security.

In section IV of the "Cyber security strategy of Romania" is defined "The national cyber security system" (NCSC) as "the general cooperation framework that brings together public authorities and institutions, with responsibilities and capabilities in the field, in order to coordinate actions at national level for ensuring the security of the cyber space, including through cooperation with the academic and business environment, professional associations and non-governmental organizations ”.

The NCSC's mission is to ensure the elements of knowledge, prevention and counteracting of the threats, vulnerabilities and risks specific to the cyber space that can affect the security of the national cyber infrastructures, including the management of the consequences (Decision no. 271/2013, section VI).

In order to fulfil the objectives of the present strategy, the NCSC functions as a unitary and efficient mechanism for interinstitutional relations and cooperation, in order to adopt and apply with speed of decisions (Decision no. 271/2013, section VI).

The NCSC constitutes the platform for cooperation and harmonization of CERT capabilities existing at national level, taking advantage of the tools offered by them, and will act to strengthen the expertise in the field of cyber risks, by stimulating synergies between the different action plans in the field of cyber security (military-civil, public-private, governmental and non-governmental) (Decision no. 271/2013, section VI).

6. Discussion, and Conclusions

Currently anyone can be the target of a cyber-attack, and the most important state institutions are usually the first ones targeted. The weak point remains the human factor, the user of the computer system. That is why in any strategy of "Cybersecurity" its awareness and training from the point of view of computer security plays a vital role.

In this context, it is necessary for the human factor to have a culture of cyber security if he/she is a user of a computer system, to know the risks and their counteracting solutions (the level being obviously differentiated according to the user).

Once formed, the human resource must be maintained in the institution, and for this the IT sector must be properly budgeted, the wage benefits must be comparable to the private one. At the same time, the optimal level of licensed equipment (software/ hardware) including viable antivirus solutions must be ensured.

At European level, the Council has established a framework that allows the Union to impose specific restrictive measures to deter and respond to cyber-attacks that pose an external threat to the EU or its Member States. This decision allows for the imposition of sanctions on persons or entities that: are responsible for cyber-attacks or cyber-attack attempts, who provide financial, technical or material support for such attacks or who are involved in or associated with them (European Council, Council of the European Union, 2019).

At the national level, Romania has developed an effective defence mechanism against cyber-attacks, Romania's Cyber Security Strategy being part of the European cyber defense effort.

The National Cyber Security Incident Response Center (CERT-RO) and the Cyberint National Center (CNC) within the Romanian Intelligence Service are interconnected with similar European institutions.

Romania has taken steps for the correct transposition within the legislative framework of the European directives (for example: the adoption of the law no. 362/2018 on ensuring a high common level of security of the networks and information systems, transposes into the national legislation the Directive (EU) 2016/1148 (NIS) of the European Parliament and of the Council of 6 July 2016 on measures for a high common level of security of networks and information systems in the Union) but this effort must have a permanent character in ensuring the legal norms, to combat the phenomenon.

At the same time, SRI, through Cyberint, carries out "awareness" activities for entities that are exposed to threats with an impact on national security and makes public materials that contribute to the strengthening of the security culture (eg the guide of good practices for cyber security) (Cyber Security Guide, Romanian Intelligence Service).

The fact that so far no attacks have been reported with major impact on central and local public institutions, strategic companies with state and / or private capital or critical

infrastructure elements, denotes that the strategy adopted by Romania is a viable one, but that must be upheld constantly depending on the dynamics of the threats.

1. References

Badea-Mihalcea, A. (2019). People and Machines: Dealing with Human Factor, *Considerations on challenges and future directions in cybersecurity,* Cyber Security National Cyberint Center, Romania, Romanian Association for Information Security Assurance (RAISA), Romanian National Computer Security Incident Response Team (CERT-RO) and the National Cyberint Center

Birta, C. F., (2017, July 2017)*, How the Internet is used by terrorists*, Intelligence Magazine, Romanian Intelligence Service, https://intelligence.sri.ro/cum-este-utilutil-internetul-de-teroristi/ accessed: 14.04.2020

Cyberint National Center, (2018, December 7), *Cyber defense. What we didn't know about the Cyberint National Center*, https://intelligence.sri.ro/defensiva-cibernetica-ce-nu-stiam-despre-centrul-national-cyberint/ accesat la data: 13.04.2020

Denning, D. E. (2001). *Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy. Networks and netwars: The future of terror, crime, and militancy*

Essomba, M., (2017, July 27), Cybersecurity Trends Magazine, https://cybersecuritytrends.ro/page/12/?s accessed:14.04.2020

Gaftea. V., Cybersecurity Becomes from a Trend, a Fact, *Considerations on challenges and future directions in cybersecurity,* Cyber Security National Cyberint Center, Romania, Romanian Association for Information Security Assurance (RAISA), Romanian National Computer Security Incident Response Team (CERT-RO) and the National Cyberint Center

Moldovan, A., (2016, December 22,), *The Internet as an instrument of terror. The network of fear*, Intelligence Magazine, Romanian Intelligence Service, https://intelligence.sri.ro/internetul-ca-instrument-al-terorii-reteaua-fricii/ accessed: 14.04.2020

Romanian National Computer Security Incident Response Team - CERT-RO, (2018), *Threats evolution in romanian cyberspace.* https://www.cert.ro/vezi/document/cert-ro-cyberthreats-2018, accessed: 14.04.2020.

Romanian National Computer Security Incident Response Team - CERT-RO, (2017), *Threats evolution in romanian cyberspace*. https://www.cert.ro/vezi/document/cert-ro-cyberthreats-2018 accessed: 14.04.2020.

Sînpetru, V., Pisargiac, C., (2019), Threats and Challenges. A National Cyber Security Perspective, *Considerations on challenges and future directions in cybersecurity,* Cyber Security National Cyberint Center, Romania, Romanian Association for Information Security Assurance (RAISA), Romanian National Computer Security Incident Response Team (CERT-RO) and the National Cyberint Center

Sînpetru, V., (2020, January 15), *Virtual targets. The stages of the cyber-attack,* Intelligence Magazine, Romanian Intelligence Service. https://intelligence.sri.ro/tinte-virtuale-etapele-atacului-cibernetic/ accessed: 13.04.2002

Trivilini, A., The Internet, between terrorism and opportunities, *Cybersecurity Trends* 4/2016

The French Government, (2020), *Cybercrime*, https://www.gouvernement.fr/risques/cybercriminalite accessed: 10.04.2020,

The General Directorate of Security and Prevention of the Federal Interior Public Service, Belgium, (2020), *Cybercrime*, https://www.besafe.be/fr/themes-de-securite/cybersecurite/cybercriminalite/en-general accessed: 10.04.2020

Romanian Intelligence Service, (2020), *Cyberintelligence***,** https://www.sri.ro/cyberint accessed: 13.04.2020

Romanian Intelligence Service, *Cyber Security Guide*, https://www.sri.ro/assets/files/publicatii/ghid_de_securitate_cibernetica.pdf accessed: 13.04.2020

National Agency for Informational Security Systems, *Main Threats*, https://www.ssi.gouv.fr/administration/principales-menaces/ accessed: 10.04.2020

European Council, Council of the European Union, (2019), https://www.consilium.europa.eu/en/policies/cybersecurity/ accessed: 14.04.2020

ENISA (European Union Agency for Cybersecurity), (2019, December), *State of vulnerabilities 2018/2019. Analysis of Events in the life of Vulnerabilities* https://www.enisa.europa.eu/publications/technical-reports-on-cybersecurity-situation-the-state-of-cyber-security-vulnerabilities accessed: 13.04.2020

Decision no. 271/2013 approving the Cyber Security Strategy of Romania and the National Action Plan on the implementation of the National Cyber Security System