

REPORT DOCUMENTATION PAGE

*Form Approved
OMB No. 0704-0188*

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.
PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE (DD-MM-YYYY) 21-04-2020	2. REPORT TYPE Master of Military Studies (MMS) thesis	3. DATES COVERED (From - To) AY 2019-2020
--	--	---

4. TITLE AND SUBTITLE Cybersecurity in Romania	5a. CONTRACT NUMBER N/A
	5b. GRANT NUMBER N/A
	5c. PROGRAM ELEMENT NUMBER N/A

6. AUTHOR(S) Geanin, Stoian (Major)	5d. PROJECT NUMBER N/A
	5e. TASK NUMBER N/A
	5f. WORK UNIT NUMBER N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) USMC Command and Staff College Marine Corps University 2076 South Street Quantico, VA 22134-5068	8. PERFORMING ORGANIZATION REPORT NUMBER N/A
--	--

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S) N/A

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

In the last decades, Romania has experienced a rapid evolution of communications and cyber technologies, which brings a more interconnected society, and the migration of public services and private business into the cyberspace. Along the development process of the cyber technology, Romania must take measures to ensure security in cyberspace, yet it still has long way to reach a high level of security. The legal framework in cybersecurity is unclear and insufficient, education and research are at low levels, and there are no clear responsibilities for developing a comprehensive cybersecurity system. All of this creates a low level of cybersecurity, with the low capability to react to medium or high-level cyber-attacks. There are real threats in cyber space either from state actors like Russia or non-state actors, who can disrupt Romanian Public institutions or deny access of citizens to essential services.

15. SUBJECT TERMS
Cybersecurity, Cyber-attack

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON	
a. REPORT	b. ABSTRACT	c. THIS PAGE			USMC Command and Staff College	
Unclass	Unclass	Unclass	UU	45	19b. TELEPHONE NUMBER (Include area code) (703) 784-3330 (Admin Office)	

*United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, VA 22134-5068*

TITLE:
Cybersecurity in Romania

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

AUTHOR:
Geanin Stoian
Major, Romanian Naval Infantry


AY 2019-2020

Mentor and Oral Defense Committee Member: Dr. Brandon Valeriano

Approved:  _____

Date: _____ April 21, 2020 _____

Oral Defense Committee Member: Lt.Col. Brian McLean

Approved:  _____

Date: _____ April 21, 2020 _____

Oral Defense Committee Member: Mr. Donald Bishop

Approved: _____

Date: _____ April 21, 2020 _____

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENT AGENCY. REFERENCES TO THIS RESEARCH SHOULD INCLUDE THE FOREGOING STATEMENT.

QUOTATION FROM, ABSTRACTION FROM, OR REPRODUCTION OF ALL OR ANY PART OF THIS DOCUMENT IS PERMITTED PROVIDED PROPER ACKNOWLEDGEMENT IS MADE

EXECUTIVE SUMMARY

Title: Cybersecurity in Romania

Author: Geanin Stoian Major, Romanian Naval Infantry

Thesis: The Romanian cyber domain is unsafe and unsecure due to the lack of clear legislation, of investment in education and training, research and innovation. Romania must initiate realistic and urgent measures to increase the security of its cyber domain, like creating a comprehensive legal framework and investing in infrastructure, education, and research. In the absence of this measures Romanian cyberspace will remain vulnerable to cyberattack and also will create an environment for cybersecurity incidents and a transit place for outside cyber-attacks.

Discussion: In the last decades, Romania has experienced a rapid evolution of communications and cyber technologies, which brings a more interconnected society, and the migration of public services and private business into the cyberspace. Along the development process of the cyber technology, Romania must take measures to ensure security in cyberspace, yet it still has long way to reach a high level of security. The legal framework in cybersecurity is unclear and insufficient, education and research are at low levels, and there are no clear responsibilities for developing a comprehensive cybersecurity system. All of this creates a low level of cybersecurity, with the low capability to react to medium or high-level cyber-attacks. There are real threats in cyber space either from state actors like Russia or non-state actors, who can disrupt Romanian Public institutions or deny access of citizens to essential services.

Conclusions: By investing in infrastructure, education, and research, combined with creating a comprehensive legal framework, Romania will reduce its vulnerabilities in the cyber domain and will create solutions to avoid cyberattacks or react as needed, in order to limit the effects of cyber-attacks and ensure continuity to its essential services.

Table of Contents

DISCLAIMER	ii
EXECUTIVE SUMMARY	iii
Introduction	1
Where does Romania stand now?	2
Background.	2
Conceptual framework	2
European context.....	6
NATO context.....	6
National legislative framework	7
Human resources and education.....	10
Innovation and research.....	12
Cyberspace in military domain	12
Enemies and threats	15
Strategically motivated actors	15
Financially motivated actors (Cyber Crime)	17
Ideologically motivated actors (Hacktivism)	19
How should Romania improve cybersecurity	19
Update legislation framework	20
Management of hardware and software	20
Develop comprehensive cyber-risk management process.....	20
Institutionalized education.....	21
Cyber Hygiene Training programs.....	22
Invest in research and development	23
Private public cooperation.....	24
Military domain.....	26
Assesment	27
Conclusions	29
Notes	31
Bibliography.....	34

List of Figures

Figure 1: Household connected to Internet in Romania.....	3
Figure 2: Internet user in Romania.....	3
Figure 3: Questioning regarding Romanian cyber legal Framework.....	9
Figure 4: Children using social media	11
Figure 5: Cybersecurity incidents in 2017.....	14
Figure 6: Types of cyber-attacks in 2017.....	15
Figure 7: Achieving the Secured Cyberspace process.....	29

Acknowledgments

I want to thank the Marine Corps University (MCU), the place where my understanding of the military and international environment had increased, due to professionalism of instructors and to the high level and challenging curriculum. Now I can say that I see the world through a new perspective, a perspective that is broader and much more realistic. Also, I would like to bring thanks to my mentor and my military faculty for their guidance and patience in completing this research.

Introduction

During the past few decades, the world has lived in a digital age. The development of communications and information technologies like smart phones, satellite communications, high speed processing computers, high speed data transfer technologies, and the expansion of the internet it is making the world more interconnected. Public institutions and private businesses have transferred their activities in the digital realm, financial transfers can be made from cafés with a swipe and a touch of the smartphone, social applications have changed today's societal behavior; all of these are just a few advantages of the development of communications and information technologies. On the other hand, the digital age hasn't brought only benefits, it has also brought some challenges, because along with technological advancements, actions of malintent have appeared in cyberspace. The possibility of cyber criminals hampering with the network system of a public or private institution, that plays the role of a critical infrastructure, where damages may result in huge losses of data, sensitive information, pecuniary losses, or even denial of essential services, is just one example of threat to cyberspace.

With these existing threats in mind, and the increasing number of cyber-attacks determined governments from all over the world to acknowledge and engage the security of cyberspace. For example, like France, Germany and Great Britain, who initiated security policies and cyber security strategies for improvement in 2011. Other countries started earlier, as a result of a direct threat to their national security, like the US, who published their first national cyber strategy in 2003, or Estonia who published its first cyber strategy in 2008, after experiencing a cyber-attack from Russia in 2007.¹

Romania began adopting cyber security measures in 2013, but has done so mainly in reaction to the European Union. The European Union's cybersecurity strategy was adopted in 2013, setting strategic objectives (developing cyber defense capabilities, reducing

cybercrime, adoption of international policy on cyberspace) to be taken by Member States.²

In the same year, Romania adopted the Romanian Cyber Security Strategy (SSCR), to be “in line with the steps taken at EU and NATO level.”³ Which brings up the question: Has Romania effectively developed cyber security efforts to mitigate current threats?

The Romanian cyber domain is unsafe and unsecure due to the lack of clear legislation, of investment in education and training, research and innovation. Romania must initiate realistic and urgent measures to increase the security of its cyber domain, like creating a comprehensive legal framework and investing in infrastructure, education, and research.

This paper’s research methodology centers on the review of studies conducted by Romanian government institutions, and the Romanian cyber domain academic community. It also includes a review of annual reports from 2017 and 2018 of institutions dealing with cybersecurity, in order to build a realistic understanding of the current cyber situation in Romania. Additionally, the methodology includes a review of international literature regarding the cyber domain in order to understand the existing threats in cyber space, and determine which are the ones that are of greatest importance to Romania. The purpose is to create a realistic view of the current state of Romanian cyber security and determine remaining risks and threats for the future. With these issues revealed, in the final chapter, the paper proposes measures and directions to improve the security environment in cyberspace.

Where does Romania stand now?

Background.

Throughout the previous two decades, cyber space has experienced a rapid evolution in Romania. It started with a slow dial up connection in the beginning of the twenty-first century, and two decades later, Romania was ranked in the top ten of countries with the highest fixed broadband,⁴ with 75.7% of Romanian households connected to the internet

(Figure 1), and 89.4% of Romanians as users in 2019 (Figure 2).⁵ The percentage of internet user is high if we compare with United Kingdom who has 90% of population using Internet,⁶ or Germany who has 94% of population using Internet.⁷ This development has generated new opportunities for both public and private sectors, but it has also brought new challenges in terms of vulnerabilities, threats, and security.

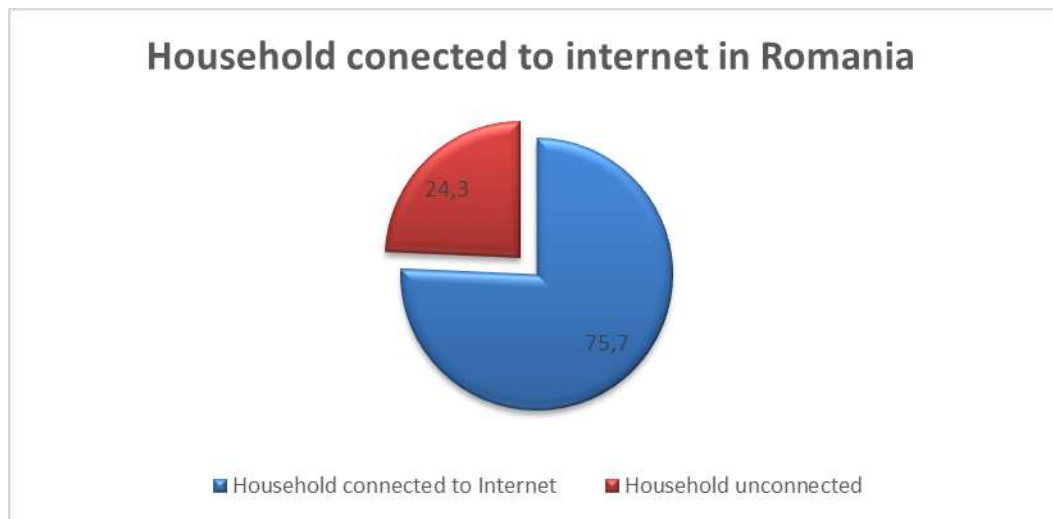


Figure 1: Household connected to Internet in Romania

Source: "Population Access to Communications and Information Technologies," National Institute of Statistics, December 2019, http://www.insse.ro/cms/sites/default/files/field/publicatii/accesul_populatiei_la_tehnologia_informatiei_si_comunicatiilor_romania_2019.pdf.

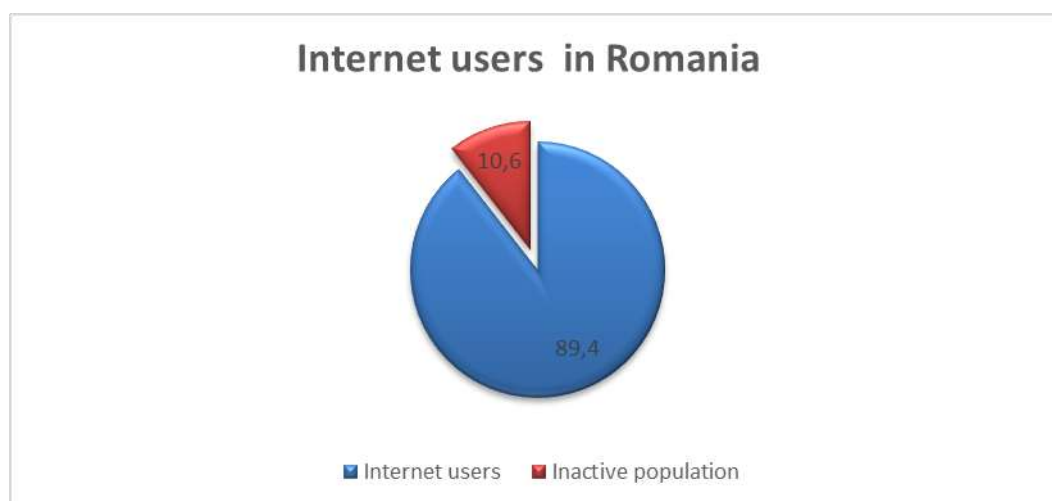


Figure 2: Internet user in Romania

Source: "Population Access to Communications and Information Technologies," National Institute of Statistics, December, 2019, http://www.insse.ro/cms/sites/default/files/field/publicatii/accesul_populatiei_la_tehnologia_informatiei_si_comunicatiilor_romania_2019.pdf

To make it even more challenging, along the informatization process, Romania has never had a defined strategy for the implementation of technological development, apart from choosing the most affordable network systems and terminals. This has led to a hybrid infrastructure throughout the country, with different characteristics in hardware and software, resulting in low performance. Many of the cyber defense systems used by critical infrastructure operators and public institutions are outdated and inefficient, unable to prevent cyber-attacks or ensure general security in cyberspace.⁸

As of November 2019, three mobile companies in Romania have launched 5G services, using Ericsson 5G technologies, which brings additional capability to the cyberspace domain. The 5G network provides new opportunities, in conjunction with the IPv6 protocol adoption. It will increase exponentially the volume of data transferred in these networks; it will also increase the speed of transfer up to 10Gbps. It will reduce the latency up to one millisecond, and, at the same time, will reduce the energy consumption. All these benefits will lead in the near future to the development and expansion of the internet of things (IoT), resulting in an increased load on infrastructure, due to the high data transfer rate in 5G networks. On the other hand, the 5G networks will also bring new challenges, for example it can easily extrapolate the current situation of malware infection of multiple IP devices or networks for DDoS attacks: increasing the number of interconnected devices will increase the critical mass of potential devices taken over in a Botnet network to initiate stronger attacks, and at a much higher speed. From this perspective the cybersecurity domain has to keep up the pace and adapt in order to confront new challenges.⁹

During the early stages of digital transformation, Romanian government institutions focused on closed networks, without being interconnected or requiring an internet connection. But the last decade has brought particular requirements that aimed to interconnect and open those networks for transparency, and for development in the social and

economic environment. These interconnections happened in conjunction with a growing diversity and complexity of threats from cyberspace,¹⁰ and have raised the need for specific measures to develop and maintain a secure cyberspace.

Conceptual framework.

Over the last decade, the Romanian academic and policy community has developed a larger interest in the cyber domain, conducting research and publishing papers to better define the cyber environment as well as its expanding effects on Romanian society and national security. The Romanian academic community is defined by, PhD and professors from the top universities of Romania such as National defense University, Police Academy, National university of Political Studies and Public Administration, and technological universities, who conduct research in cyber security domain. There are also professional associations dedicated to promote the cybersecurity culture, like *The Romanian Association for Information Security Assurance* who promote the cybersecurity culture and to fight against the cybercrime phenomenon. From the academic environment most, notable scholars and leaders in cybersecurity research are Ph.D. Ioan Mihai Cosmin, a cybersecurity and cybercrime researcher, professor, trainer and conference speaker. He is an Associate Professor at "Al. I. Cuza" Police Academy, "Carol I" National Defense University, the Polytechnic University of Bucharest, Romania, and Honorary Professor at the CT University, India, where he is teaching disciplines related to information technology, cybersecurity, and cybercrime. Also, Ph.D. Victor Adrian VEVERA cybersecurity researcher, he is an Associate Professor at "Mihai Viteazul" National Intelligence Academy, he was a former leader of General Directorate for Intelligence and Internal Security, former director of CERT-RO, and currently a member of the National Institute for R&D in Informatics.

The Romanian academic community, defines cyber space as a “virtual environment, generated by the cybernetic infrastructures. It includes the processed informational content,

stored or transmitted, and also the unfolded actions of the users.”¹¹ The academics recognized the possibilities that developments in the cyber domain will continue to further develop the society and the economy, but they also acknowledge the risks that this development will bring to the security of the nation. Cyber security is defined as “the state of normality resulting from the application of a set of proactive and reactive measures that ensure the confidentiality, integrity, availability, of electronic information, resources and services, public or private in cyberspace.”¹² When the academic community refers to proactive and reactive measures it refers to general policies, security standards, risk management, training, and technological solutions. Also, when it comes to threats against Romanian cyberspace and how those threats are going to influence the society, the academic community has a separate approach for different actors. For example, looking at the threat posed by extremists, and terrorists it is considered “low, in relation to Romania's national security.”¹³ But when the academic community addresses the financial motivated actor and state actors, it considers that these actors determine an „increasing level of cyber threat.”¹⁴

European union context.

The European Union (EU) did not have a coherent unified policy towards cyber security until 2013, “with relevant actors working independently from each other in areas as distinct as law enforcement, critical information infrastructure protection, and defense.”¹⁵ But the sustained increase in cyber-attacks on critical information infrastructures and on personal and commercial data led the European Union to expand its role as a major actor in cyber security when it published its first cyber security strategy in 2013, aiming to establish for more cohesive policy across member states. The strategy aimed at improving cyber resilience to threats of member states and the private sector, as well as lowering the overall level of cyber-crimes. The policy also encouraged cooperation between all actors involved (member

state and private sector), increased investment in cyber defense capabilities and capacities needed to respond to attacks, and instigated more engagement with international partners.¹⁶

Since 2013, cybercrime has become one of the most important priorities of EU, with legislative progress achieved in 2016 in the adoption of the Network and Information (NIS) Directive.¹⁷ The NIS Directive specifically addresses essential service providers and digital service providers, establishing requirements and measurements for effective security assurance. The directive has also introduced cyber incident reporting obligations for both the public and private sectors. The European Union policies and legislation drive actions of member states in cyber security, as the requirements they establish are mandatory for all members and must be implemented in the national law. As an example, the NIS Directive states that “Each Member State shall adopt a national strategy on the security of network and information systems,”¹⁸ and set as the deadline the date of 9 May 2018. This requirement resulted in Romania as the *Law on ensuring a high common level of security of computer networks and systems*.

NATO context.

Being part of NATO since 2004, Romania followed NATO steps in the military side of cyberspace. The wake-up call for NATO was the cyber-attack against Estonia in 2007, when over a three-week period, government institutions, internet service providers, financial institutions, and small businesses were all targeted and disrupted. The cyber action exposed vulnerabilities and demonstrated the prospects of a cyber-attack to create extensive damage, if intended. This attack also led to a significant strengthening of cyber defense capabilities, institutions, and legislation throughout NATO.¹⁹ At Lisbon summit in 2010, NATO declared its interest in the cyberspace domain, stating that “in order to ensure NATO’s permanent and unfettered access to cyberspace and integrity of its critical systems, we will take into account the cyber dimension of modern conflicts in NATO’s doctrine and improve its capabilities to

detect, assess, prevent, defend and recover in case of a cyberattack against systems of critical importance to the Alliance.”²⁰ Starting from this point, NATO developed defense policies for cyber security and created the NATO Computer Incident Response Capability. An important milestone in developing cyber-defense capabilities was in 2016, at the Warsaw summit, when the Alliance officially declared that cyber space can be considered an operational dimension, stating that “Now, in Warsaw, we reaffirm NATO’s defensive mandate, and recognize cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea.”²¹ By recognizing cyberspace as a separate domain, it means that NATO will start developing strategies and plans for along with the creation of specialized structures to engage the cyberspace domain, at least at the same level as other existing domains.

National legislative framework

As part of the European Union since 2007, Romania has followed European directives in matters of cybersecurity. The European Union's cybersecurity strategy was adopted in 2013, setting strategic objectives (developing cyber defense capabilities, reducing cybercrime, adoption of international policy on cyberspace) to be taken by all Member States.²² To ensure cybersecurity compliance, in the same year, “Romania adopted the Romanian Cyber Security Strategy (SSCR).”²³

The SSCR has as purpose to define and maintain a safe cyberspace, in the benefit of its people, economic environment, and its society, by ensuring security in cyber space with a focus on four major goals.²⁴ The first is to establish a *theoretical and conceptual framework to ensure cybersecurity*.²⁵ This step is supposed to establish a minimum-security requirement in order to develop the cooperation between public and private sectors. The second goal is the development of *risk management and reaction capabilities*,²⁶ which involves the creation of cybernetic structures meant to provide early warnings and initiate reactions to

cyberattacks. The third goal aims to *promote* security methods in the cyber-domain by developing institutionalized training programs in cyber hygiene and cyber defense. The final goal is to establish cooperation within the international community for common cyber defense in the European Union and NATO.

Lacking clear measurable objectives defined in time, Romania failed to make any substantial progress in cyber security development up until 2018. As an example, the next law regarding the cyber security domain was not adopted until 2018. That year, the *Law on ensuring a high common level of security of computer networks and systems* was implemented. The intent of the law was to create a cohesive national framework for providing cybersecurity and improving the reaction to cyber-attacks, in accordance with the European NIS directive. It addresses essential service providers and digital service providers, assigning them responsibilities for ensuring cyber security and reporting cyber incidents. It also addresses the standards and the minimum-security technical requirements to be implemented by service providers in order to increase the level of cyber security. The responsibility for establishing the technical requirements and standards is given to CERT-RO, who was nominated as the national authority in cyber security. The Law should strengthen the security of cyber space, but the lack of specific timelines for its application resulted in debilitating delays to its effectiveness. For example, “the minimum requirements for implementing security in networks”, “the list of essential services providers” and all other legal documents that support the applicability of the Law on ensuring a high common level of security of computer networks and systems, had not been elaborated or approved yet.²⁷

A 2018 survey conducted by the European Institute in Romania showed that 85% of subjects declared that the national law regarding cyber security is unclear and insufficient to establish clear cyber security objectives in public institutions.²⁸ This study proves that the

legal framework did not effectively strengthen the nation’s cybersecurity, but instead created confusion among public institutions.

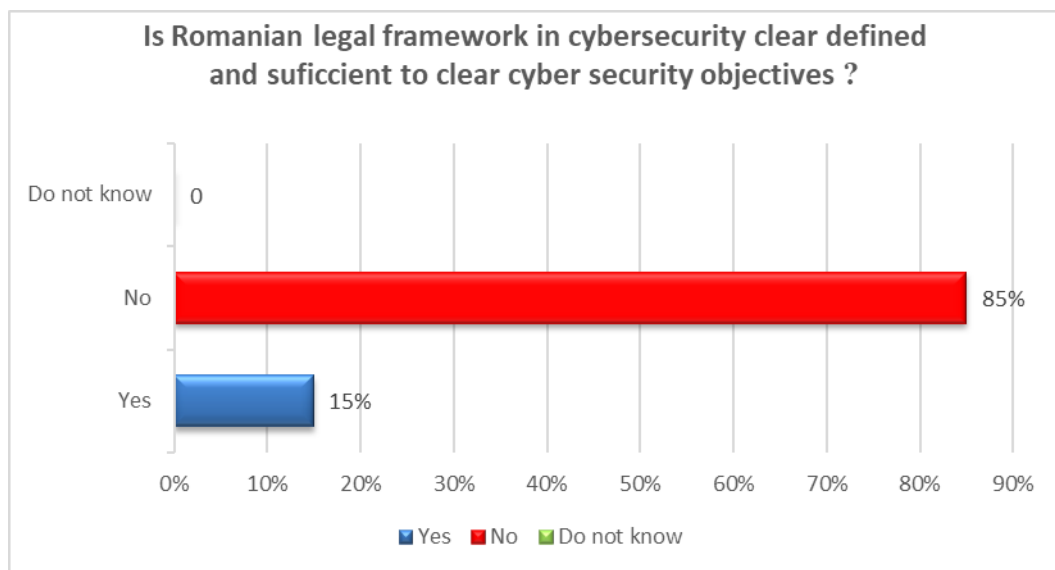


Figure 3: Questioning regarding Romanian cyber legal Framework

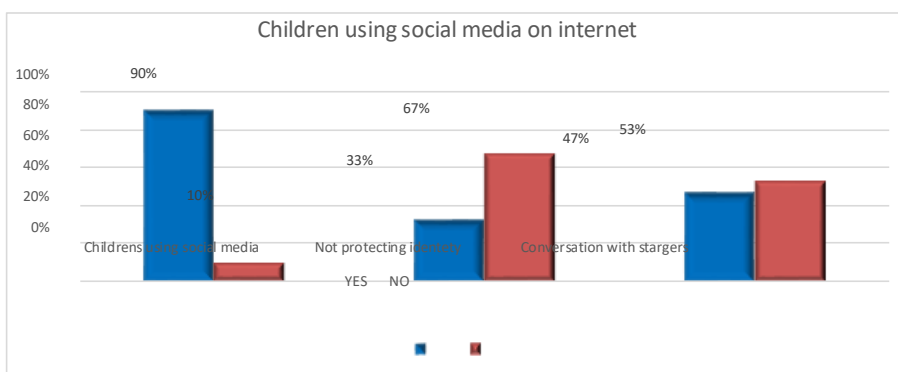
Source: Ioan Mihai Cosmin, “Current challenges in cyber security domain,” Bucuresti 2018, http://ier.gov.ro/wp-content/uploads/2018/10/SPOS-2017_Studiul_4_FINAL.pdf

In addition to the incomplete laws in cyber domain, in Romania there is also a lack of public institutions that should handle the cyber security. At this time there are only six structures providing cybersecurity, under the form of CERT (Cyber Security Incident Response Center). A general center at the national level is CERT-RO, which is the coordinator for the other CERT entities. CERT-MIL, which belongs to the Defense Ministry, is focused on cyber security within the military domain, CERT-INT deals with cybersecurity of Internal Affairs, ROCSIRT is the academic version of CERT handling cybersecurity for the national teaching system, and CYBERINT supervises cybersecurity for the Romanian Intelligence Service. Out of these, only CERT-RO and CYBERINT publish information about current cyber security threats. However, their sites are not well known, so the information provided does not have a major impact in improving the nation’s understanding of credible cyber threats. Moreover, CERT-RO is supposed to be a coordinator for the other CERT entities, but it does not share an identified command relationship with them, resulting in poor inter-agency cooperation.²⁹

Human resources and education.

The lack of a highly qualified workforce in cyber security is an issue worldwide from which, unfortunately, Romania is no exception. The few capable cyber security professionals were coopted by the private sector, due to the uneven financial gain.³⁰ In order to better respond to the national demand for a quality workforce in cyber security, the Romanian Intelligence Service, through the National CYBERINT Center, together with the Ministry of Education and the IT industry, has already initiated steps for developing educational programs in cyber security. In 2018 postgraduate studies and master studies were implemented in national universities with technical backgrounds.³¹

The situation in high schools is different though; cyber security has not yet been largely introduced as part of the curriculum. This situation is quite alarming, since cyber hygiene elements are absolutely mandatory for every internet user, especially for young ones. A study conducted by Romanian Association for Information Security Assurance, shows that “over 90% of children, between 9 and 18 years old, were using social networks and 33% of them were not protecting their real-life identity, while 47% of children had online



conversations with strangers.”³²

Figure 4: Children using social media

Source: Ana, Badea Mihalcea, “People and Machines: Dealing with Human Factor in Cyber Security”, In *Considerations on challenges and future directions in*

cybersecurity, Edited by Ioan Cosmin Matei, 143-154, (Craiova, SITECH Publishing, 2019), <https://www.sri.ro/assets/files/cyberint/CybersecurityRO2019.pdf>, 151

As the study shows, the number of children and teenagers using an internet connection is very high, hence the need for protection and education. Taking into consideration their innocence and naivety, they become easy targets for different means of cyber-crime. And yet, even after this study, only four high schools in Romania out of the existing 1534 (2016) introduced cyber hygiene programs as an experimental program in 2018.³³ A little too late, as the SSCR has directed this issue since 2013.

As for training the current employed force, the public sector has failed to achieve any noticeable progress. Even in institutions abundant in technological innovations, training is scarce and not made a priority, and yet it is expected from the employees to act as if they should know everything there is to know about cyber security. A study conducted by the European Institute in Romania among the employees of various public institutions showed that 85% of subjects stated that the institutions they work for hadn't run a training or awareness program regarding cybersecurity.³⁴ The result indicates the lack of training in cyber hygiene and cyber security, which makes the employees vulnerable for cyber-attack. One of the most common methods of cyber-attacks is social engineering, which is targeting the human layer of an infrastructure. People without any kind of training in cyber security become easy targets, diminishing the institution's cyber security and the national cyber space, since the public institutions are interconnected.

Innovation and research.

According to the European Commission's report, Romania invests the lowest amount on cyber innovation (including cybersecurity), capability development, and research out of all member states.³⁵ It would be a fair assessment to say that both the migration of human resources and the lack of research projects conducted has resulted in a lack of sustainable solutions for the cyber security of public institutions. The lack of Romania's government

investment in research is balanced at a national level by the private sector's innovation in cyber. The local private companies' corporations, which consider cyber security as a priority objective, invest in research and focus on current and future solutions to improve cyber security.

Among the private sectors of cyber security, the leader in cyber security research and development is BITDEFENDER, a Romanian company specialized in cyber security which provides security solutions for computer networks. There are also smaller specialized local and corporate companies that can provide support in achieving a good cyber security capability. But these companies invest for their own interest and they do not provide for the security of public institutions unless they have been contracted, which they currently have not been.

Cyber space in military domain.

Following NATO politics, in its own rhythm, Romania by signing the Warsaw agreement, considers Cyberspace as a military domain, and in December 2018, the defense minister created the Cyber Defense Command within the Romanian military under the command of the General Staff. The new structure became responsible for developing and ensuring cyber resiliency to military infrastructures and services. With the creation of the Cyber defense command, each service rebranded a few of its communications units as "Communications and cyber defense", and directly tasked them with cyber defense responsibilities.

Granting the fact that this change was an important step in cyber defense development, the Romanian military service is still a long way from achieving a coherent cyber security environment. The lack of specialized personnel for this field is no different than anywhere else in the Romanian military. Tasking people that have a technological background with new cyber responsibilities does not transform them overnight into cyber

warriors, and it does not solve the problem of needing specialized skills and personnel. The army lacks substantial cyber training or hygiene and still relies on Classified Documents Protection, an outdated training program that does not meet the needs of current-day cyber security threats.

Even though the Romanian Ministry of Defense still relies on segmented networks with physical connection between systems (no Wi-Fi), and no internet connection, there are still vulnerabilities to be exploited in case services are disrupted. The “attack on the Iranian refining uranium installations”³⁶ in 2010 is example of a cyber-attack on a closed network. The attacker used a malware named “Stuxnet” which was delivered through USB device, which had been designed to be autonomous, since there was no internet connection to control its action remotely.³⁷ The Stuxnet example thus shows that a closed network can still be targeted and disrupted if cybersecurity measures are not put in place to mitigate apparent vulnerabilities.

Romania has taken some efforts in strengthening its national cybersecurity, from both legal and institutional points of view. However, the country has not yet achieved a secure cyber domain. At the moment, Romania cannot react, prevent, or counter a medium and/or a high level cyber threat with maximum efficiency.³⁸ In addition to this, according to the annual report of CERT-RO, Romania is both a country who “generates cybersecurity incidents and provides a transit place for outside attackers, due to vulnerable or compromised system for national cyber space.”³⁹

When it comes to offensive operations in cyberspace or persistent engagement, Romania's military or institutions didn't publish any kind of framework or strategy. There could be two reasons for that. First, it may be classified which limits the research of this paper. Either, offensive operations and persistent engagement are not an option for Romania,

since Romania's main focus in its security strategy is national defense (inside its borders), and public order and cohesion.⁴⁰

Enemies and threats

Cyber-attacks against citizens, public institutions, and private institutions have increased both in terms of quantity and complexity of the attacks, resulting in a 2018 cyber security risk assessment rating of “HIGH” by CYBERINT.⁴¹ According to a CERT-Ro report in 2017, 138,217,026 cyber-security alerts were collocated and processed throughout of Romania. They affected 2.9 million IP addresses, representing 33% from the total of IP assigned to Romania, a substantial increase from the 25% reported in 2016.⁴² And the number could be much higher, since in 2017 a clear law of reporting and transmitting information about cybersecurity incidents was nonexistent.

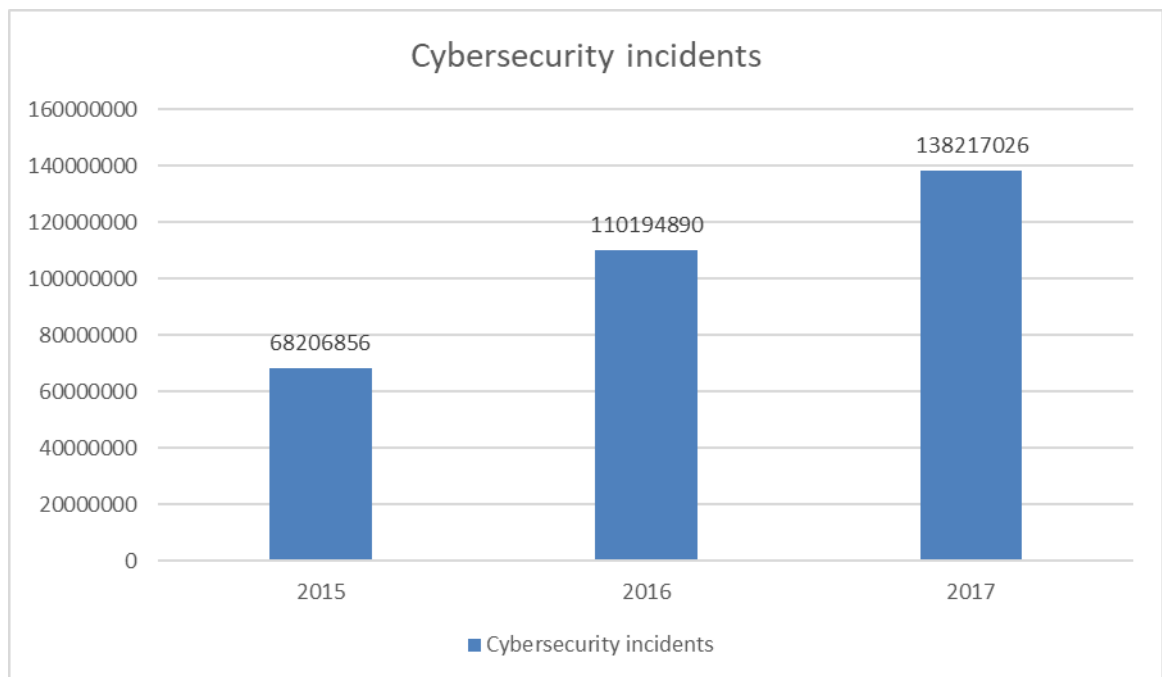


Figure 5: Cybersecurity incidents in 2017

Source: “Report regarding Cyber threats in 2017,” Cyber Security Incident Response Center Romania, Bucharest, May, 2018, <https://cert.ro/vezi/document/raport-alerte-2017>

The increasing number of cyber security incidents shows how bad the situation actually is, at the same time revealing the need for urgent measures to be taken in order to increase the security in cyber space.

The Romanian Intelligence Service claimed that there are three types of actors responsible for cyber-attacks in Romania: strategically motivated actors (state actors), financially motivated actors (cyber-crime), and ideologically motivated groups (hacktivists).

Strategically motivated actors.

State actor sponsored attacks target public institutions within the Foreign Affairs and Defense domains, with the main objective of extracting information of strategic interest. These types of attacks have a high level of technological complexity, which allow the attacker to remain undetected for a long period of time through difficult signature tracing. The most common attack used by strategically motivated actors is Advanced Persistent Threat (APT), which represents 12% of the cyber-attacks, in Romania⁴³

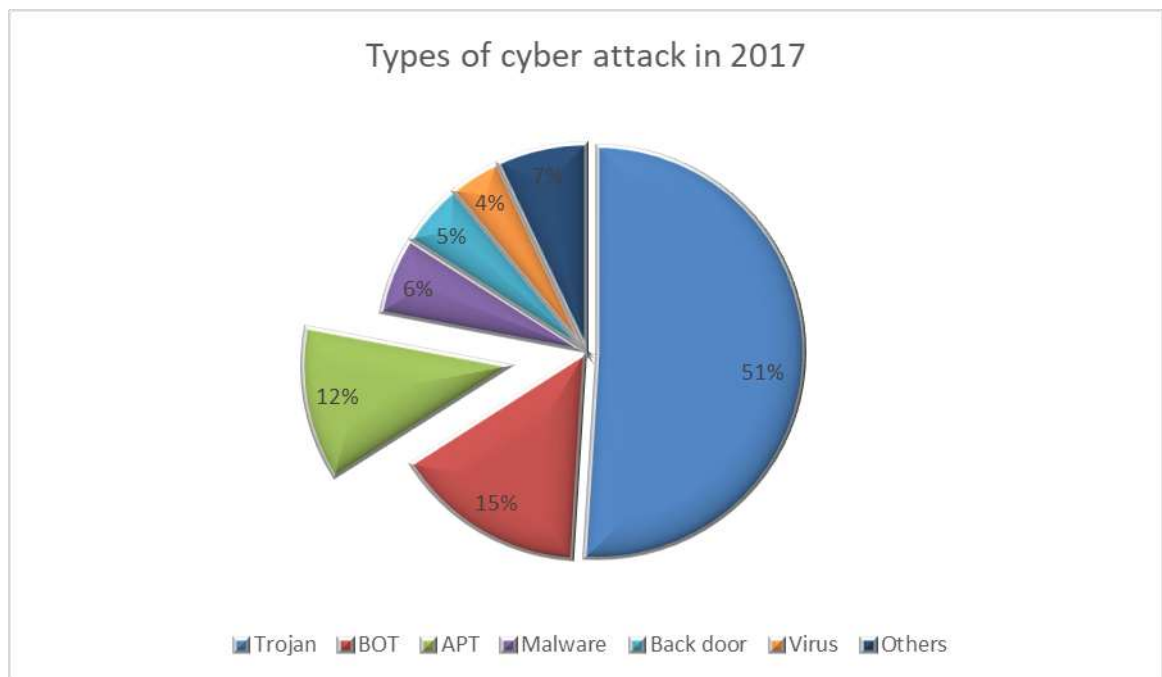


Figure 6: Types of cyber-attacks in 2017

Source: “CYBERINT Bulletin 1st semester 2018,” Romanian Intelligence Service, July, 2018, <https://www.sri.ro/assets/files/publicatii/BULETIN-CYBERINT-20x20cm.pdf>

Among the strategic APT cyber-attacks, which targeted Romanian institutions, National Cyberint Center reported and investigated the ATP28, MiniDuke, and Snake, which were of high technology development malwares and targeted government institutions, like the foreign affairs ministry, defense ministry, as well as the energy, communications, and education sectors. The attacks used procedures like spearfishing, social engineering, backdoors exploiting. Also, it was reported the Red October, a medium level technology malware that targeted governmental scientific research organizations, used the same procedures of attack like spearfishing and social engineering.⁴⁴

It is difficult to identify which specific state actors are involved in cyber-attacks, especially since they do not publicly accept responsibility. Taking into account Romania's geographical position, the fact that it is part of the EU and NATO, and the actions that Russia has taken in the previous years to include the annexation of Crimea and the destabilization in Ukraine, it is a fair assessment that the biggest threat to Romania's national security and cyber security is currently Russia.

Russia has demonstrated its cyber capabilities and the will to use them. It has conducted cyberattacks in order to disorient western states and to distract them from conventional military activities. It has combined cyberwarfare with conventional warfare, the most recent example being the cyber-attacks used in Ukraine against the government, media, and energy infrastructure.⁴⁵ An analysis of the Ukrainian crisis may offer a better understanding of the threat that Russia poses to other countries, including Romania. At the onset of the conflict, Russia used cyber space for intelligence and reconnaissance, combined with conventional military operations, to isolate the Crimean Peninsula. Hereafter, it used cyber-attack to degrade military units and capabilities. As an example, in 2016 Russia used an android malware to infect Ukrainian artillery targeting apps, providing information on

their position and enabling Russian assets to accurately attack them. Then, Russia triggered a cyber campaign to degrade the Ukrainian infrastructure and disrupt the country's essential services. In October 2014, using the malware Black Energy 3, Russia gained access to power plants and thus was able to put them offline. Apart from its direct cyber actions, Russia also conducted large disinformation campaigns in cyberspace, using social media and trojan infections to redirect users to propaganda web sites that supported Russian intent and initiated dissension throughout Ukrainian politics.⁴⁶ "Russia is a rogue actor in the digital domain,"⁴⁷ conducting cyber actions of espionage and disruptive techniques to create chaos and disinformation against former Soviet states, including Romania.⁴⁸

Financially motivated actors (Cyber Crime).

Financially motivated attacks are executed by individuals or groups that are interested in obtaining significant financial gain, targeting a wide variety of entities without discrimination between public and private institutions or end-users. Romania is commonly targeted by such attacks. According to DIICOT (Direction of investigation of organized crime and terrorism) annual report, in 2017 there were 5,329 of unsolved cases of cybercrime in Romania. Additionally, 1,294 new cases emerged with an increasing number of these cyber-crimes being committed by young adults and minors.

The majority of reported cybercrime cases were of ransomware, with no specific targets and no discrimination. Beside ransomware cybercrimes, an increased number of new cases in social engineering were reported, with the *man in the middle* technique used to commit fraud. Additionally, cryptomining, and attacks targeted on the IoT have become a growing trend in cybercrime in Romania.⁴⁹

An example of Romanian cybercrime was an attack that took place in the second half of 2018, targeting the networks of inter-banking transfer and ATMs, in order to achieve financial gain. The attack was conducted by the group known as Cobalt Strike, and an open

source tool was used. Consequently, there were considerable financial losses, which affected banking institutions not only in Romania but also in Europe and Asia.⁵⁰

Another disturbing event happened in May 2019, when multiple hospitals from Romania were targeted by a cyber-attack trying to encrypt data and deny access. As the investigation of the attack was done by SRI, the conclusion was that the attack originated from China.⁵¹ The event was catalogued as a cybercrime since the involvement of Chinese authorities could not be directly proven.

These examples easily demonstrate that cyber-attacks conducted by nonstate actors can have a huge impact on Romania's national security, as they can be directed at critical infrastructures, thus denying vital assets like financial and medical services.

Ideologically motivated actors (Hacktivism).

Ideologically motivated cyber-attacks are carried out by hacktivist groups, cyber terrorist groups, or independent hackers. The evolution of this kind of attack is dynamic and unpredictable, being driven by political or social events which present interest for these groups. The hacktivist cyberattack aims to access information and databases with the purpose of revealing them to the public, or changes the content of web pages to express and publicize their beliefs. When it comes to terrorist groups, there were no cyber-attacks with major impact on Romania's cyber security, but these groups do effectively use cyberspace for supporting propaganda activities, recruitment, and dispersed radicalization.⁵²

As a result of not having an established cohesive cyber defense strategy, cyber-attacks are in great number throughout Romanian cyber space, especially in the cyber-crime domain. They can negatively impact national security, since these cybercrimes are not discriminatory on type of target. At the same time, because of Romania's membership in NATO and EU alliances, as well as its strategic geographic position, Romania is a commonly

identified target for state actors who hope to conduct espionage and disruption campaigns through cyber means.

How should Romania improve cybersecurity?

Update legislation framework.

The 2013 cyber security strategy should be updated, or rewritten, in order to adapt to the new challenges present in the cyber domain and to mitigate the current and future threats to the national cyberspace. The SSCR should acknowledge the reality of the current status of Romanian cyber security and recognize its weaknesses in order to develop feasible solutions. These should be focused on having a safe cyberspace for both public and private institutions while establishing clear and measurable objectives of the cyber security. With a comprehensive SSCR, that includes direction, actions, and responsibilities to be initiated at the national level; the country may achieve the goal of drawing public and private sector activities together to strengthen the security of the cyber space.

The objectives of this particular strategy should be to defend cyberspace from current and possible threats, to deter aggression in cyber space, and to be continuously aligned to the new emerging technology challenges developing in the cyber domain. All these objectives should contain direction and active measures to be achieved through the instrumentality of the responsible institutions.⁵³

Another element of an effective legal framework is establishing clear public security policies that will contain rules (laws), standards, and plans to protect cyber space and react in case a cyber incident occurs. This plan of action should follow some basic guidelines in order to establish clear responsibilities in defining norms and standards, coordination and implementation. The plan should promote safe cyberspace while respecting the freedom and the liberties of the citizens, establishing legal framework to impose minimum security

standards to service providers, operational measures (plans) in responding to an incident, and ensuring services continuity along with backup storage facilities.⁵⁴

Management of hardware and software.

Since there were previously no coherent policies on developing IT infrastructure in Romania, it is imperative that all public institutions conduct an inventory of current assets. The technological infrastructure has to be continuously analyzed, monitored, and evaluated in order to identify hardware and software types, capabilities, and resources.⁵⁵ By doing this inventory, it will be much easier to identify a vulnerable system and the needs for updates or migration between software. For example, there are still systems in some public institutions that use the updated version of windows, or the unsupported one like Windows Xp, or institutions that use unlicensed cybersecurity tools. These types of non-regulated systems generate vulnerabilities and are prone to cyber-attacks that could impact the entire public sector.

At the same time, a library or a register at the national level should be created, with trustworthy software for all types of requirements; a safe place from where this software can be purchased should also be established. Additionally, there should be minimum standard requirements for systems to be purchased, in order for them to be safely integrated in public institutions networks.⁵⁶

Develop comprehensive cyber-risk management process.

It is mandatory that a cyber security risk management process is developed in public institutions, which will enable identifying critical systems and data/information that are of national interest and at risk. These systems/data attract attention and can become targets of cyber-attacks conducted by state or nonstate actors, depending on the interest they have.⁵⁷ Once the critical system/data have been identified, the next step would be to acknowledge the existing threats and the means of a possible attack, based on previous experiences. The

succeeding actions should be identifying and analyzing the vulnerabilities of the system and finding adequate solutions to diminish or remove these vulnerabilities. Alongside identifying vulnerabilities, an analysis of the consequences can determine the most affected services, for both the institution and the national level, what the costs to restore those services are, and the necessary solutions that need to be taken in case of attack. As a final step, the public institutions should conduct a cost-effective analysis, in order to identify the most efficient solutions and their effects. Consequently, they should decide upon the most viable solution to be applied, in order to identify the possible vulnerabilities or reduce and/or accept associated risks.⁵⁸

A good example of risk management model is the Ortwin Renn model, in which the risks are divided in 3 groups (intolerable, tolerable and acceptable) depending on the impact that the risk would have and the probability of its occurrence.⁵⁹ By using this model, the public institutions can identify the risks that need immediate attention, and prioritize resources to address them. The risk management process will allow a better view of the network's security needs, and it will also allow a smart and prioritized investment in cyber security and infrastructure solutions.

Institutionalized education.

Since there is a lack of human resources specialized in cyber security, the only way to increase this resource is by institutionalized education. Even if some colleges in Romania previously started educational programs in cybersecurity, it is not currently enough to supply the demand. Education in cyber security should start at least from the high school level, since more than 90% of teenagers are using an internet connection. By doing so, the benefits would be of considerable size. First, it will increase the security culture in cyber space and the users will learn how to correctly use the internet resources, how to distinguish the accurate ones, and how to protect themselves from the threats of cybercrime. Secondly, in the long term, it

may increase the interest in cyber security and they could choose to follow a specific educational program or a cyber security career.⁶⁰

Institutionalized cyber education should become a priority to the educational systems and it should be implemented as soon as possible. The curriculum and the teaching methods should match the requirements and the realities of the cyber domain. This means that beside the theoretical part of the curriculum, a portion of the course should be focused on practical, real life simulations. By implementing institutionalized cyber education, technical abilities in cyber security can be developed, leading to fundamental skills in recognizing and avoiding cyber-attacks.⁶¹

Cyber Hygiene Training programs.

Adjacent to institutionalized education, Romania should give great importance to cyber hygiene training programs for public institutions. As discussed in the first chapter, a significant percent of the employees working in public institutions have no idea about cyber security, which creates a human layer vulnerability in cyber security. The purpose of cyber hygiene training is to offer the employees a general introduction to common cyber threats, as well as ways to avoid attacks of any kind. It also creates a security culture, by understanding particular responsibilities and by acknowledging the importance of each individual in creating a safe cyber environment for the institution. Cyber training improves the security level by diminishing the human layer vulnerabilities of cyber security.⁶²

This training should be continuous and adapted for each institution, according to the roles and responsibilities of the employees, but it should include general information about authorized access in systems and networks, updating software, how to recognize and detect threats (like phishing mails), and procedures for action in case of a discovered threat. In order to be efficient, the training should be followed by a theoretical evaluation and by simulating cyber incidents/attacks, to determine the security level knowledge, and the institutions'

vulnerability. The evaluation will help improve training, so the employees will raise their level of knowledge and skills in recognizing threats and avoiding them.⁶³

The training should be periodical, in the direction of keeping a high level of awareness, and it should also be permanently adapted to the new threats that occur in cyberspace.

Invest in research and development.

The National Strategy for Research, Development and Innovation was published in Romania in 2014, establishing some general objectives for economic, societal, and technological growth by the means of supporting innovations,⁶⁴ yet, it does not have any objective or direction in cyber security research and development. The migration of public and private institutions to a cyber world of activity and the increasing tendency of online interactions, raise the need for prioritizing the research and the development of the security tools in the cyber domain, to ensure the continuity of all services. Furthermore, the evolutionary feature of the cyber domain and the new technologies and protocols emerging on the market (for example 5G technologies) require a much higher level of attention to given cyber security solutions.⁶⁵

In this context, Romania should start investing in research and development programs to evolve and discover new security solutions to keep the cyber domain safe. Since it has fallen behind in comparison to the European countries in the research domain, as shown in chapter one, with the only current research being conducted in the private sector, Romania should create a public-private partnership in developing solutions against cyber threats. Investing in the cyber security and allocating funds for the research and innovation domain, must be established at the government level and respected. The budget for research and innovation should be increased to 2% from GDP (as stipulated in the National Strategy, of research and development), instead of 0.18% from GDP as is was in 2019⁶⁶. The research in

cyber domain should focus on identifying vulnerabilities and threats to the Romanian cyber space, and developing technological solutions and security policies to mitigate the threats, and reduce vulnerabilities.⁶⁷

Private public cooperation.

Cyberspace has no physical boundaries between public institutions and private institutions, in fact most of the communications infrastructure is developed by private companies.⁶⁸ Moreover, the internet services providers are private companies. The governmental institutions are the only authorities that can investigate cyber incidents, in order to protect the citizens. In addition to this, cyber-attacks are nondiscriminatory between systems belonging to public institutions, private companies or individuals themselves. All these facts lead to the need for a private-public cooperation that can help ensure a safe cyberspace.⁶⁹

A model of a private public partnership that could be employed is the Institutional model described by European Union Agency for Network and Information Security. This kind of partnership can be built and used to carry out activities related to the protection of infrastructures that provide essential services. Public institutions are tasked with critical infrastructure protection by a legal act (crisis management/ emergency act), but the private sector that operates those infrastructures has a better knowledge and understanding of how to address the inherent security needs. This reinforces the need of public-private cooperation, better enabling the goal of securing critical infrastructure from cyber threats. This kind of public-private cooperation involves actors from public institution tasked with infrastructure security (for example internal affairs minister), and actors from all the private sectors identified as essential services providers (energy, health care, transportation, financial and banking, etc.) The governance of this partnership is based on an institutional hierarchy, specific to the governmental institutions. However, working groups under the umbrella of this

type of partnership are governed by the private sector, with the private sector making the strategic decisions that are then addressed by the public institutions. Funding is primarily provided through the government, so private sector participation can be voluntary. Developed public-private partnerships can better provide services like incident handling and crisis management, research and analysis, information exchange, standards definition, technical evaluation, help desk support, security audits, and risk analysis operations, to improve the cyber security domain at lower cost.⁷⁰

Military domain.

In addition to the suggestions listed before for improving the national cybersecurity, in the military domain specific measures need to be taken, in order to develop a cyber defense capability that can detect and react in the face of state actors' cyber-attacks. Rebranding communications units and giving them cyber security tasks is not a viable solution. Indeed, the coms units have security measures to protect their assets and communications, and sometimes these may overlap with cybersecurity measures, but that does not mean they will be able to ensure cyber security to military networks. These units have the same strength and the same knowledge that they had before rebranding, and instead of creating a capability, the military service creates a vulnerability. As a solution, cyber defense centers should be created at critical points of the networks, to ensure cyber security.⁷¹

Moreover, since the military does possess the means to create a mass of specialists through the Military Technical Academy, short to medium specialization trainings should be conducted, beside the long-term programs, thus creating enough specialized personnel for the cyber centers. Also, the military domain should take into consideration changing its personnel policies, in order to maintain and attract specialized skills. The cyber personnel are not a gun fighting machine, and to complete their mission and responsibilities, they do not need to be physically trained to run 'x' miles and do 'y' pushups. The military service requires brains

and knowledge, so it is a good idea to change recruiting qualifications for the specialized cyber personnel. In addition to this, to maintain specialized personnel in its structure, the military service should match the financial benefits for the cyber personnel, so that it is competitive to the private sector employees.

Cyber exercises, as well involving the armed forces in general military exercises with a cyber component, could also be good solutions to test cybersecurity and find vulnerabilities and ways to mitigate. Also, participating in exercises that reveal the threats to cyber security will rise the general level of awareness of military personnel regarding cyber security importance.⁷²

Also, because the military domain is a classified area, the tendency is to work isolated, with no connection to other public or private institutions. The cyber security information should not have a high classification level, it can even be unclassified, and the military cyber structures should partner with public institutions and private companies to increase the cyber defense capabilities.⁷³

Assessment

A way to achieve a secure cyberspace is to implement the mentioned solution in a logical sequential order as in figure 7, starting with the first step of creating a *comprehensive legal framework*. The legal framework is the base of creating secure cyberspace because is the driver for establishing network security standards and norms, security policies, and clear responsibilities for creating a safe cyberspace. The second step is the *Hardware and software management*. After establishing the standards, and norms, the process should continue with the identification of network systems outside the standards, and the vulnerabilities and gaps that this system creates in cyberspace security. The third step is to apply the *risk management matrix* to the identified vulnerabilities and gaps, to create priorities. Priorities

are necessary, since the resources are limited, and the investment in infrastructure will come gradually.

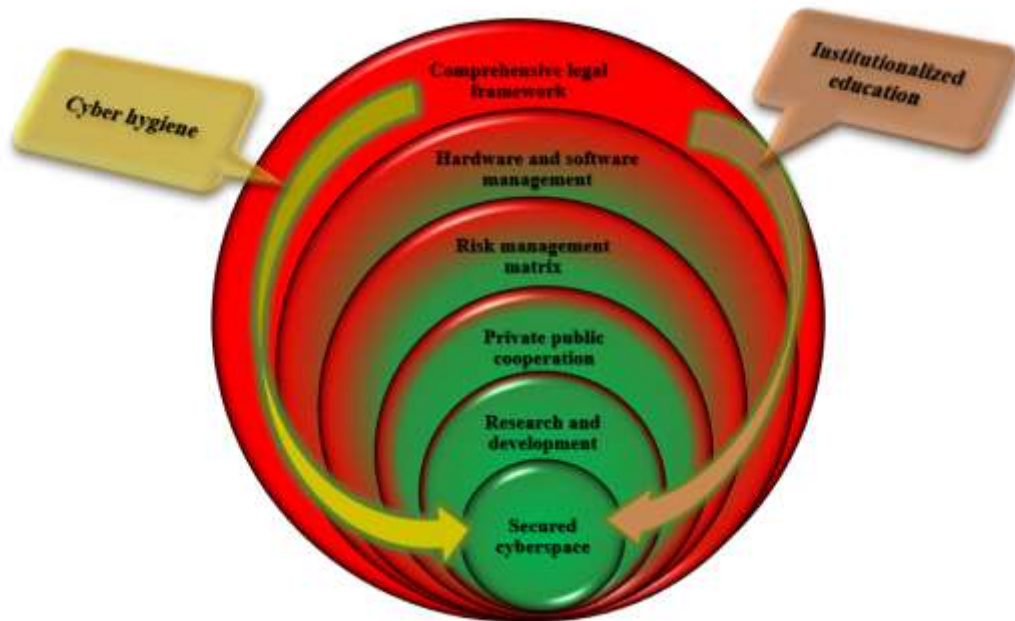


Figure 7: Achieving *the Secured Cyberspace* process.

The fourth step will be to create a *private-public cooperation* partnership. Since cybersecurity is not only a state interest, the creation of the private-public partnership will increase the resources (financial and human components), in addressing the vulnerabilities and the threats to cyberspace. The final step is the *research and development* of solutions to address the vulnerabilities, tools to negate threats and ensure the security of cyberspace.

The *Cyber hygiene* training programs, an *institutionalized education*, are rather continuous processes, than defined steps in achieving a secure cyberspace. *Cyber hygiene* should start as soon as the legal framework is established. It has to be continued and adaptive to respond and deny new vulnerabilities and threats. Also, the *institutionalized education* programs must be developed and started at the same time with the legal framework, so it can create a specialized workforce in the cybersecurity domain.

Conclusions

The research showed that Romania has started a process to strengthen cybersecurity at both national and institutional levels, making some efforts in the right direction, but the reality shows that the slow pace and sometimes incomprehensible measures cannot create a secure cyberspace. The reason for unsafe cyberspace lies in the intricate and vague legislation, combined with the lack of education, research, and no security policies. All of this issue creates from Romanian cyberspace a safe haven for cyber-attacks against both public institutions and private companies, including the Romanian citizens.

Also, another point that the research paper shows, in the second chapter, even though Romania is a small country, there are threats to its security posed by financially motivated actors, who are indiscriminate about their targets as long as they can obtain profit. Also, being part of NATO and EU, combined with its geographical position, draws more threats towards Romania from state actors, especially from Russia. These threats cannot be ignored for long. The damage that cybercrime produces and the indiscriminatory targeting are a menace not only to cyber space, but also to national security and the citizens. The aggressive Russian policy in the former soviet states raises the question of whether or not Romania is a safe country. All of these threats draw the urgent need to strengthen the security of the cyber space.

In order to create a better security environment in cyber space, Romania should invest in infrastructure and create a comprehensive management of hardware and software to exert improved control over its network, along with a risk management matrix. Also, Romania should create specialists in cyber and develop methods of ensuring security by investing in education and research. And create a comprehensive legal framework which contains clear objectives and responsibilities well defined in time.

On account of living in a digital era where everything tends to migrate in the cyber realm, cyber security is crucial in order to ensure national security, economic growth, and societal development. Romania has made progress in developing a safe cyberspace, yet its cyber security is precarious because of unclear legislative frameworks, lack of specialized personnel and training in cybersecurity, and low investments in research and development. Also, the unclear relations between specialized institutions have contributed to a general weakness in cybersecurity throughout the country.

Romania's cyber space is unsafe and creates opportunities for different actors to conduct cyberattacks. However, by taking comprehensive measures, Romania can improve its cyber security, reduce its vulnerabilities, and create solutions to avoid or react as needed, in order to limit the effects of cyber-attacks and ensure continuity of its essential services.

Notes

¹ VIRGIL TOȘA, “Cybersecurity Strategies of Some Geopolitical Actors”. The Impact of social-economic and technological evolution at national, European and global level, No.4 (2015), Vol.4., <https://ssrn.com/abstract=2661977>

² Costel Chiuci, “Challenges in Cyber Resilience for Public Administration”, In *Considerations on challenges and future directions in cybersecurity*, Edited by Ioan Cosmin Matei, 229-242,(Craiova, SITECH Publishing,2019), <https://www.sri.ro/assets/files/cyberint/CybersecurityRO2019.pdf>, 231

³ Romanian Cybersecurity strategy, <https://lege5.ro/App/Document/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>

⁴ According to Speed test Global index accessed at <https://www.speedtest.net/global-index>, accessed on 29.12.2019, 07.18

⁵ Romanian National Institute of Statistics, “Population Access to Communications and Information Technologies”, December, 2019, http://www.insse.ro/cms/sites/default/files/field/publicatii/accesul_populatiei_la_tehnologia_informatiei_si_comunicatiilor_romania_2019.pdf

⁶ <https://www.ons.gov.uk/businessindustryandtrade/itandinternetindustry/bulletins/internetusers/2018>

⁷ <https://www.statista.com/statistics/380514/internet-usage-rate-germany/>

⁸ Mihai Ioan Cosmin, Costel Chiucia and Gabriel Marius Petrica, “Current challenges in cybersecurity domain-Impact and the contribution of Romania”, (Bucharest) 2018, http://ier.gov.ro/wp-content/uploads/2018/10/SPOS-2017_Studiul_4_FINAL.pdf

⁹ Stănculescu Virgilius, “The Communications Future. 5G Between Benefits and Cybersecurity Challenges”, In *Considerations on challenges and future directions in cybersecurity*, Edited by Ioan Cosmin Matei, 59-78,(Craiova, SITECH Publishing,2019), <https://www.sri.ro/assets/files/cyberint/CybersecurityRO2019.pdf>, 61

¹⁰ Romanian government, The ministry of communication and the information society, Cyber Security Study CCS 146, (Bucharest, 2015), https://www.comunicatii.gov.ro/wp-content/uploads/2016/02/CyberSec_nov2015.pdf

¹¹ Victor Adrian VEVERA. "CYBER SPACE, ROMANIA AND THE NEW THREATS". In *Studia Securitatis* 2:61-67,2016, <https://www.ceeol.com/search/article-detail?id=469929>

¹² Victor Adrian VEVERA. "CYBER SPACE, ROMANIA AND THE NEW THREATS".in *Studia Securitatis* 2:61-67,2016, <https://www.ceeol.com/search/article-detail?id=469929>

¹³ Victor Adrian VEVERA. "CYBER SPACE, ROMANIA AND THE NEW THREATS". In *Studia Securitatis* 2:61-67,2016, <https://www.ceeol.com/search/article-detail?id=469929>

¹⁴ Victor Adrian VEVERA. "CYBER SPACE, ROMANIA AND THE NEW THREATS". In *Studia Securitatis* 2:61-67,2016, <https://www.ceeol.com/search/article-detail?id=469929>

¹⁵ Carrapiço, Helena ; Barrinha, André., European Union cyber security as an emerging research and policy field, *EUROPEAN POLITICS AND SOCIETY*, 2018, VOL. 19, NO. 3, 299–303,

¹⁶ Carrapiço, Helena ; Barrinha, André., European Union cyber security as an emerging research and policy field, *EUROPEAN POLITICS AND SOCIETY*, 2018, VOL. 19, NO. 3, 299–303,

¹⁷ Carrapiço, Helena ; Barrinha, André. / The EU as a coherent (cyber)security actor?. In: *Journal of Common Market Studies*. 2017 ; Vol. 55, No. 6. pp. 1254-1272.

¹⁸ Directive (EU) 2016/1148 OF THE European Parliament and of The Council of 6 July 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

¹⁹ NATO StratCom Riga Latvia, “2007 Cyber-attacks on Estonia”, <https://www.stratcomcoe.org> › file › fid

²⁰ North Atlantic Treaty Organization (NATO). (2010). Lisbon Summit Declaration. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Lisbon, available at: https://www.nato.int/cps/en/natohq/official_texts_68828.htm, accessed on: 20 February 2018.

²¹ North Atlantic Treaty Organization (NATO). (2016). Warsaw Summit Communiqué. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw, https://www.nato.int/cps/en/natohq/official_texts_133169.htm,

²² Costel Chiuci, “Challenges in Cyber Resilience for Public Administration”, In *Considerations on challenges and future directions in cybersecurity*, Edited by Ioan Cosmin Matei, 229-242,(Craiova, SITECH Publishing,2019), <https://www.sri.ro/assets/files/cyberint/CybersecurityRO2019.pdf>, 231

-
- ²³ Romanian Cybersecurity strategy, <https://lege5.ro/App/Document/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>
- ²⁴ Romanian Cybersecurity strategy, <https://lege5.ro/App/Document/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>
- ²⁵ Romanian Cybersecurity strategy, <https://lege5.ro/App/Document/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>
- ²⁶ Romanian Cybersecurity strategy, <https://lege5.ro/App/Document/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>
- ²⁷ *Law on ensuring a high common level of security of computer networks and systems*, <https://lege5.ro/App/Document/gmytiobyga2a/legea-nr-362-2018-privind-asigurarea-unui-nivel-comun-ridicat-de-securitate-a-retelelor-si-sistemelor-informatic>
- ²⁸ Mihai Ioan Cosmin, Costel Chiuci and Gabriel Marius Petrica, “Current challenges in cybersecurity domain-Impact and the contribution of Romania”, (Bucharest) 2018, http://ier.gov.ro/wp-content/uploads/2018/10/SPOS-2017_Studiul_4_FINAL.pdf
- ²⁹ Romanian government, The ministry of communication and the information society, “Cyber Security Study CCS 146”, (Bucharest, 2015) <https://www.comunicatii.gov.ro/wp-content/uploads/2016/02/CyberSecnov2015.pdf>
- ³⁰ Romanian Intelligence Service. *CYBERINT Bulletin 1st semester 2019*, Bucharest, July, 2019, <https://www.sri.ro/assets/files/publicatii/buletin-cyber-sem-1-2019.pdf>
- ³¹ Ana, Badea Mihalcea, “People and Machines: Dealing with Human Factor in Cyber Security”, In *Considerations on challenges and future directions in cybersecurity*, Edited by Ioan Cosmin Matei, 143-154, (Craiova, SITECH Publishing, 2019), <https://www.sri.ro/assets/files/cyberint/CybersecurityRO2019.pdf>, 151
- ³² Ana, Badea Mihalcea, “People and Machines: Dealing with Human Factor in Cyber Security”, In *Considerations on challenges and future directions in cybersecurity*, Edited by Ioan Cosmin Matei, 143-154, (Craiova, SITECH Publishing, 2019), <https://www.sri.ro/assets/files/cyberint/CybersecurityRO2019.pdf>, 151
- ³³ Romanian Intelligence Service. *CYBERINT Bulletin 1st semester 2019*, Bucharest, July, 2019, <https://www.sri.ro/assets/files/publicatii/buletin-cyber-sem-1-2019.pdf>
- ³⁴ Mihai Ioan Cosmin, Costel Chiucia and Gabriel Marius Petrica, “Current challenges in cybersecurity domain-Impact and the contribution of Romania”, (Bucharest) 2018, http://ier.gov.ro/wp-content/uploads/2018/10/SPOS-2017_Studiul_4_FINAL.pdf
- ³⁵ Constantin Ioan , “Innovation and Research - Current State, Trends and Challenges”, In *Considerations on challenges and future directions in cybersecurity*, Edited by Ioan Cosmin Matei, 79-84, (Craiova, SITECH Publishing, 2019), <https://www.sri.ro/assets/files/cyberint/CybersecurityRO2019.pdf>, 79
- ³⁶ Green James A, “Cyber Warfare, A multidisciplinary analyses”, (New York, Routledge, 2015) 20
- ³⁷ Green James A, “Cyber Warfare, A multidisciplinary analyses”, (New York, Routledge, 2015) 20
- ³⁸ Mihai Ioan Cosmin, Costel Chiucia and Gabriel Marius Petrica, “Current challenges in cybersecurity domain-Impact and the contribution of Romania”, (Bucharest) 2018, http://ier.gov.ro/wp-content/uploads/2018/10/SPOS-2017_Studiul_4_FINAL.pdf
- ³⁹ Cyber Security Incident Response Center Romania. *Report regarding Cyber threats in 2017*, Bucharest, May, 2018, <https://cert.ro/vezi/document/raport-alerte-2017>
- ⁴⁰ Romania’s National Defense Strategy, https://www.presidency.ro/files/userfiles/Strategia_Nationala_de_Aparare_a_Tarii_1.pdf
- ⁴¹ Romanian Intelligence Service. *CYBERINT Bulletin 1st semester 2019*, Bucharest, July, 2019, <https://www.sri.ro/assets/files/publicatii/buletin-cyber-sem-1-2019.pdf>
- ⁴² Cyber Security Incident Response Center Romania. *Report regarding Cyber threats in 2017*, Bucharest, May, 2018, <https://cert.ro/vezi/document/raport-alerte-2017>
- ⁴³ Romanian Intelligence Service. *CYBERINT Bulletin 1st semester 2019*, Bucharest, July, 2019, <https://www.sri.ro/assets/files/publicatii/buletin-cyber-sem-1-2019.pdf>
- ⁴⁴ Viorel SÎNPETRU and Cătălina PISARGIAC, “Threats and Challenges. A National Cyber Security Perspective”, In *Considerations on challenges and future directions in cybersecurity*, Edited by Ioan Cosmin Matei, 187-200, (Craiova, SITECH Publishing, 2019), <https://www.sri.ro/assets/files/cyberint/CybersecurityRO2019.pdf>, 189

- ⁴⁵ Foxall Andrew, “Putin’s Cyberwar: Russia’s Statecraft in the Fifth Domain”, (The Henry Jackson Society, May 2016), https://www.stratcomcoe.org/online_library
- ⁴⁶ Valeriano Brandon, Benjamin Jensen and Ryan C Maness, “Cyber Startegy the Evolving character of power and coercion, (New York, Oxford University press, 2018), 140-141
- ⁴⁷ Valeriano Brandon, Benjamin Jensen and Ryan C Maness, “Cyber Startegy the Evolving character of power and coercion, (New York, Oxford University press, 2018), 141
- ⁴⁸ Valeriano Brandon, Benjamin Jensen and Ryan C Maness, “Cyber Startegy the Evolving character of power and coercion, (New York, Oxford University press, 2018), 118
- ⁴⁹ Romanian Direction of Investigation of Organized Crime and Terrorism, “Annual report 2017”, (Bucharest, April 2018), http://diicot.ro/images/documents/rapoarte_activitate/raport.2017.pdf
- ⁵⁰ Viorel SÎNPETRU and Cătălina PISARGIAC, “Threats and Challenges. A National Cyber Security Perspective”, In *In Considerations on challenges and future directions in cybersecurity*, Edited by Ioan Cosmin Matei, 187-200, (Craiova, SITECH Publishing, 2019), <https://www.sri.ro/assets/files/cyberint/CybersecurityRO2019.pdf>, 189
- ⁵¹ “CERT-RO shows origins of hackers responsible for cyber-attacks in Romania” news release, June 21, 2019 <http://www.ziare.com/internet-si-tehnologie/atac-cibernet/cert-ro-de-unde-provin-cele-mai-multe-atacuri-informatic-e-asupa-administratiei-publice-din-romania-sri-chinezii-au-atacat-spitalele-din-bucuresti-1566368>
- ⁵² Viorel Sînpetru and Cătălina Pisargiac, “Threats and Challenges. A National Cyber Security Perspective”, In *In Considerations on challenges and future directions in cybersecurity*, Edited by Ioan Cosmin Matei, 187-200, (Craiova, SITECH Publishing, 2019), <https://www.sri.ro/assets/files/cyberint/CybersecurityRO2019.pdf>, 189
- ⁵³ National cyber security strategy 2016-2021 for United Kingdom of Great Britain, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf
- ⁵⁴ National Cyber Security Strategy for Norway, <https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/national-cyber-security-strategy-for-norway.pdf>
- ⁵⁵ National Cyber Security Strategy for Norway, <https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/national-cyber-security-strategy-for-norway.pdf>
- ⁵⁶ Răzvan Bărbieru “GDPR - Enemy or Friend” In *In Considerations on challenges and future directions in cybersecurity*, Edited by Ioan Cosmin Matei, 187-200, (Craiova, SITECH Publishing, 2019), <https://www.sri.ro/assets/files/cyberint/CybersecurityRO2019.pdf>, 312
- ⁵⁷ Mihai Ioan Cosmin, Costel Chiucia and Gabriel Marius Petrica, “Current challenges in cybersecurity domain-Impact and the contribution of Romania”, (Bucharest) 2018, http://ier.gov.ro/wp-content/uploads/2018/10/SPOS-2017_Studiul_4_FINAL.pdf
- ⁵⁸ Mihai Ioan Cosmin, Costel Chiucia and Gabriel Marius Petrica, “Current challenges in cybersecurity domain-Impact and the contribution of Romania”, (Bucharest) 2018, http://ier.gov.ro/wp-content/uploads/2018/10/SPOS-2017_Studiul_4_FINAL.pdf
- ⁵⁹ Renn, Ortwin & Klinke, Andreas. “Risk Governance and Resilience: New Approaches to Cope with Uncertainty and Ambiguity” in *Risk Governance: The Articulation of Hazard, Politics and Ecology*. 19-41., September 2015, https://www.researchgate.net/publication/283736368_Risk_Governance_and_Resilience_New_Approaches_to_Cope_with_Uncertainty_and_Ambiguity
- ⁶⁰ Ana Badea-Mihalcea “People and Machines: Dealing with Human Factor in Cyber Security” In *In Considerations on challenges and future directions in cybersecurity*, Edited by Ioan Cosmin Matei, 187-200, (Craiova, SITECH Publishing, 2019), <https://www.sri.ro/assets/files/cyberint/CybersecurityRO2019.pdf>, 147
- ⁶¹ Ana Badea-Mihalcea “People and Machines: Dealing with Human Factor in Cyber Security” In *In Considerations on challenges and future directions in cybersecurity*, Edited by Ioan Cosmin Matei, 187-200, (Craiova, SITECH Publishing, 2019), <https://www.sri.ro/assets/files/cyberint/CybersecurityRO2019.pdf>, 149
- ⁶² National Cyber Security Strategy for Norway, <https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/national-cyber-security-strategy-for-norway.pdf>
- ⁶³ Ana Badea-Mihalcea “People and Machines: Dealing with Human Factor in Cyber Security” In *In Considerations on challenges and future directions in cybersecurity*, Edited by Ioan Cosmin Matei, 187-200, (Craiova, SITECH Publishing, 2019), <https://www.sri.ro/assets/files/cyberint/CybersecurityRO2019.pdf>, 150

⁶⁴ Constantin Ioan , “Innovation and Research - Current State, Trends and Challenges”, In *Considerations on challenges and future directions in cybersecurity*, Edited by Ioan Cosmin Matei, 79-84,(Craiova, SITECH Publishing,2019), <https://www.sri.ro/assets/files/cyberint/CybersecurityRO2019.pdf>, 84

⁶⁵ Constantin Ioan , “Innovation and Research - Current State, Trends and Challenges”, In *Considerations on challenges and future directions in cybersecurity*, Edited by Ioan Cosmin Matei, 79-84,(Craiova, SITECH Publishing,2019), <https://www.sri.ro/assets/files/cyberint/CybersecurityRO2019.pdf>

⁶⁶ Research gets 0,18% of GDP, same as last year. Smallest budget in research and development domain from Europe, Press release , January 2019, EDUPEDU, <https://www.edupedu.ro/cercetarea-primeste-018-din-pib-procentual-la-fel-ca-anul-trecut-in-suma-exacta-alocarea-creste-cu-380-milioane-lei/>

⁶⁷ National Cyber Security Strategy for Norway, <https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/national-cyber-security-strategy-for-norway.pdf>

⁶⁸ David R. Johnson, David G. Post, “Law And Borders: The Rise of Law in Cyberspace”, (Stanford Law Review 1367, 1996,) <https://cyber.harvard.edu/is02/readings/johnson-post.html>

⁶⁹ National Cyber Security Strategy for Norway, <https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/national-cyber-security-strategy-for-norway.pdf>

⁷⁰ European Union Agency for Network and Information Security, Public Private Partnerships (PPP), Cooperative models, November 2017, www.enisa.europa.eu

⁷¹ National Cyber Security Strategy for Norway, <https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/national-cyber-security-strategy-for-norway.pdf>

⁷² National Cyber Security Strategy for Norway, <https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/national-cyber-security-strategy-for-norway.pdf>

⁷³ National Cyber Security Strategy for Norway, <https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/national-cyber-security-strategy-for-norway.pdf>

Bibliography

Andrew Foxall, "Putin's Cyberwar: Russia's Statecraft in the Fifth Domain", The Henry Jackson Society, May 2016, https://www.stratcomcoe.org/online_library.

Badea Mihalcea Ana, "People and Machines: Dealing with Human Factor in Cyber Security", In *Considerations on challenges and future directions in cybersecurity*, Edited by Ioan Cosmin Matei, 143-154, Craiova, SITECH Publishing, 2019, <https://www.sri.ro/assets/files/cyberint/CybersecurityRO2019.pdf>.

Brandon Valeriano, Benjamin Jensen and Ryan C Maness, "Cyber Strategy the Evolving character of power and coercion", New York, Oxford University press, 2018.

Brandon Valeriano and Ryan C Maness, "Cyberwar vs Cyber Realities, Cyberconflict in the International System", New York: Oxford University Press, 2015.

"CERT-RO shows origins of hackers responsible for cyber-attacks in Romania" news release, June 21, 2019 <http://www.ziare.com/internet-si-tehnologie/atac-cibernetic/cert-ro-de-unde-provin-cele-mai-multe-atacuri-informatic-e-asupa-administratiei-publice-din-romania-sri-chinezii-au-atacat-spitalele-din-bucuresti-1566368>.

Chiuci Costel, "Challenges in Cyber Resilience for Public Administration", In *Considerations on challenges and future directions in cybersecurity*, Edited by Ioan Cosmin Matei, 229-242, (Craiova, SITECH Publishing, 2019), <https://www.sri.ro/assets/files/cyberint/CybersecurityRO2019.pdf>

Cosmin Mihai Ioan, Costel Chiucia and Gabriel Marius Petrica, "Current challenges in cybersecurity domain-Impact and the contribution of Romania", (Bucharest) 2018, http://ier.gov.ro/wp-content/uploads/2018/10/SPOS-2017_Studiul_4_FINAL.pdf

European Union Agency for Network and Information Security, Public Private Partnerships (PPP), Cooperative models, November 2017, www.enisa.europa.eu

Green James A, “Cyber Warfare, A multidisciplinary analyses”, New York, Routledge, 2015

Ioan Constantin , “Innovation and Research - Current State, Trends and Challenges”, In *Considerations on challenges and future directions in cybersecurity*, Edited by Ioan Cosmin Matei, 79-84, Craiova, SITECH Publishing, 2019, <https://www.sri.ro/assets/files/cyberint/CybersecurityRO2019.pdf>

Law on ensuring a high common level of security of computer networks and systems, <https://lege5.ro/App/Document/gmytiobyga2a/legea-nr-362-2018-privind-asigurarea-unui-nivel-comun-ridicat-de-securitate-a-retelelor-si-sistemelor-informaticice>

National Cyber Security Strategy for Norway, <https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/national-cyber-security-strategy-for-norway.pdf>

National cyber security strategy 2016-2021 for United Kingdom of Great Britain, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

NATO StratCom Riga Latvia, “2007 Cyber-attacks on Estonia”, [https://www.stratcomcoe.org/file > fid](https://www.stratcomcoe.org/file%20fid)

North Atlantic Treaty Organization (NATO). (2016). Warsaw Summit Communiqué. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw, https://www.nato.int/cps/en/natohq/official_texts_133169.htm,

North Atlantic Treaty Organization (NATO). (2010). Lisbon Summit Declaration. Issued by the Heads of State and Government participating in the meeting of the North

Atlantic Council in Lisbon, available at: https://www.nato.int/cps/en/natohq/official_texts_68828.htm.

Răzvan Bărbieru “GDPR - Enemy or Friend” In In Considerations on challenges and future directions in cybersecurity, Edited by Ioan Cosmin Matei,187-200, Craiova, SITECH Publishing,2019, <https://www.sri.ro/assets/files/cyberint/CybersecurityRO2019.pdf>,

Renn, Ortwin & Klinke, Andreas. (2015). Risk Governance and Resilience: New Approaches to Cope with Uncertainty and Ambiguity, in Risk Governance: The Articulation of Hazard, Politics and Ecology. 19-41, September 2015 https://www.researchgate.net/publication/283736368_Risk_Governance_and_Resilience_New_Approaches_to_Cope_with_Uncertainty_and_Ambiguity

Romanian Cybersecurity strategy, <https://lege5.ro/App/Document/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>

Romanian Direction of Investigation of Organized Crime and Terrorism, “Annual report 2017”, Bucharest, April 2018, http://diicot.ro/images/documents/rapoarte_activitate/raport.2017.pdf.

Romanian Government, The ministry of communication and the information society, “Cyber Security Study CCS 146”, Bucharest, 2015, <https://www.comunicatii.gov.ro/wp-content/uploads/2016/02/CyberSecnov2015.pdf>.

Romanian Intelligence Service. *CYBERINT Bulletin 1st semester 2019*, Bucharest, July, 2019, <https://www.sri.ro/assets/files/publicatii/buletin-cyber-sem-1-2019.pdf>.

Romanian National Institute of Statistics, “Population Access to Communications and Information Technologies”, December, 2019, <http://www.insse.ro/cms/sites/default/files>

/field/publicatii/accesul_populatiei_la_tehnologia_informatiei_si_comunicatiilor_romania_2019.pdf

Sînpetru Viorel and Pisargiac Cătălina,” Threats and Challenges. A National Cyber Security Perspective”, In *In Considerations on challenges and future directions in cybersecurity, Edited by Ioan Cosmin Matei, 187-200, Craiova, SITECH Publishing, 2019,* <https://www.sri.ro/assets/files/cyberint/CybersecurityRO2019.pdf>

TOȘA VIRGIL, “Cybersecurity Strategies of Some Geopolitical Actors”. The Impact of social-economic and technological evolution at national, European and global level, No.4 (2015), Vol.4., <https://ssrn.com/abstract=2661977>

Victor Adrian VEVERA. "CYBER SPACE, ROMANIA AND THE NEW THREATS". In *Studia Securitatis* 2:61-67, February 2016, <https://www.ceeol.com/search/article-detail?id=469929>

Virgilius Stănciulescu, “The Communications Future. 5G Between Benefits and Cybersecurity Challenges”, In *In Considerations on challenges and future directions in cybersecurity, Edited by Ioan Cosmin Matei, 59-78,(Craiova, SITECH Publishing, 2019),* <https://www.sri.ro/assets/files/cyberint/CybersecurityRO2019.pdf>