CYBER SECURITY.

FREEDOM VS SECURITY IN THE ONLINE ENVIRONMENT

Summary

The 9/11 events influenced the national security strategies of most states, in which terrorism was defined as the main threat, thus supporting the process of globalization, which went beyond its economic nature, when the whole world united against a single enemy, in solidarity. However, in recent times, there has been a blurring of this solidarity[1], with "competition and competitiveness between states" becoming more important[2].

At the same time, one of the pillars of globalization is the evolution of technology and, implicitly, the widespread use of the Internet, which has led to the removal of major barriers to communication, knowledge and exploration of the world and created new opportunities for development and cooperation in many areas, accelerating this process. From this perspective, the use of the Internet and facilitating access to information has, in recent times, led to the reconfiguration of relations between states, starting from the need to strengthen their role and place in international relations. Information is power, and the internet and technology provide access to information. However, this environment is dominated by threats, which are constantly and rapidly evolving, which has generated the need for security of Internet users - whether simple users, companies, organizations or states, and security measures must be taken at all levels. and by all actors involved.

The present paper has as a central element the concept of cyber security and users' perception of it, from the perspective of analyzing the relationship between freedom and security.

Cyber security is a complex and evolving field, being directly influenced by the online threats' development and diversification, which must be approached differently, depending on

[1] Monitorul Apărării și Securității, Sergiu Medar, at the Conference *Cum răspundem la crizele de securitate națională*?, 2021, video available https://www.facebook.com/monitorulapararii/videos/1136156286802705/?__so__=permalink&__rv__=related_videos, last accessed, February 2021

[2] Ibid.

the effect that threats can have on system security. If at the individual level, cybersecurity involves minimal protection measures against threats that may affect systems at a low level, in the case of institutions, organizations or states, the impact may be extensive, as critical infrastructures may be affected, which may jeopardize economic, social or political stability of a state.

Thus, at state level, cyber security is a dimension of national security, which is relevant both at national and international level. At national level, the implementation of cybersecurity measures aims precisely to protect the state and, implicitly, its citizens, and internationally, states' cybersecurity policies influence international relations, as cyberspace has become a new environment of conflict and partnerships. between states and, as a result, international relations have taken on new dimensions.

Adressing the freedom vs. security relation and the theory that "security can be balanced with other values such as freedom"[3] is not new. They are always in debate, when it comes to take the necessary specific measures for national security, within a state. The most relevant example is the adoption of the Patriot Act[4] in the United States in 2001. The document consisted of "expanding the government’s power in surveillance, investigation and detention of terrorism suspects"[5]. Although disputed over time because "some provisions were unconstitutional or allowed abuse by the authorities"[6], it was adopted in a context of crisis following the 9/11 terrorist attacks, and it was applied in the original form of until 2015, when the USA Freedom Act came into force, intended to "limit the government's authority to collect data"[7].

Currently, most countries in the world have adopted a national cybersecurity strategy, but there is the debate about the need to sign an international treaty, as more and more states and international organizations define the online environment as a common good, such as maritime or outer space for which such international documents exist. However, the models provided by

[3] Richard Ullman, “Redefining Security”, in *Security Studies. A reader*, ed. Christopher W. Hughes and Lai Yew Meng (London: Routledge, 2011), 12

[4] USA Congress, *Uniting and Strengtening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001*, https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf, last accessed, June 2021

[5] Brian Duignan. "USA PATRIOT Act." Encyclopedia Britannica, November 12, 2020 disponibil la https://www.britannica.com/topic/USA-PATRIOT-Act, last accessed, January 2021

[6] Ibid.

[7] Ibid.

the Outer Space Treaty which "prohibits malicious intervention in the exploration and peaceful use of outer space and the launching of nuclear weapons from space on Earth"[8], or by the Antarctic Treaty which limits the use of weapons ”by less than 60 degrees south latitude” [9], are not enough, so a treaty on cyberspace is far from being signed.

Regarding national legislation, the difficulties lie, similarly to the national security field, in the relationship between freedom and security, and users fear that the security measures taken may affect their freedom in cyberspace. From this perspective, Member States of the European Union have limited their measures to adopting such a legislative document, by transposing the NIS Directive into national law[10].

Based on this data, the work Cyber Security. Online Freedom Vs. Security proposes highlighting the relevant aspects in the field, from the following perspectives: analysis of the threats, risks and vulnerabilities evolution in the online environment, evaluation of the legislative framework on cyber security, both internationally and nationally, and analysis of internet users' perception on the relevant legislation and the level of their cyber security culture.

The aim of the research thesis is to identify possible solutions to reduce the cyber threats materialization, through proposals on how to approach cyber security in national legislation, in the international organizational context in which Romania finds itself, given the membership of the European Union and the NATO ally, as well as taking into account the perception of internet users about the legislation in the field.

The main objective of the research is to identify the role that cybersecurity culture can play in balancing the relationship between the need for freedom of Internet users and that of security, in the face of cyber risks and threats.

The secondary objectives aim at understanding the specific phenomena of cyber security by defining and clarifying some terms, concepts and cause-effect relations specific to the online environment.

[8] Peter Warren Singer and Allan Friedman. *Cybersecurity and cyberwar. What everyone needs to know* (New York: Oxford University Press, 2014), 186

[9] Ibid.

[10] Parlamentul European și Consiliul Uniunii Europene, *Directiva 2016/ 1148 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune*, 2016, https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32016L1148&qid=1596915362573&from=EN, last accessed, June 2021

In this context, the paper proposes the demonstration of the following hypothesis: if the level of cybersecurity culture is high, then the number of attacks in the online environment may decrease.

It is a primary, causal hypothesis[11], with two variables: an independent variable - high level of cybersecurity culture, which influences the dependent variable - decreasing the success rate of cyber threats.

The explanatory hypothesis[12] adds another intermediate variable in the relationship described above, namely balancing the relationship between the need for freedom and the one of security, with the role of effect for the independent variable and cause for the dependent variable.

In the development of this hypothesis, there are new intermediate variables that intervene in the relationship between the three described above, respectively:

(1) knowing the phenomena and threats in the online environment and (2) awareness of the need for security, as an immediate effect of the independent variable - increasing the level of cybersecurity culture;

(3) knowing and applying security measures, by each user, as a direct consequence of the second variable - balancing the freedom / security ratio.

Therefore, a high level of cybersecurity culture ensures that users are aware of online threats and of their need for security, which leads to balancing the relationship between the need for freedom and security ratio, in the perception of users who, in this context, know and can apply security measures in the online environment, thus leading to a decrease in the success rate of cyber attacks.

Increasing the level of security culture can be achieved through cyber security education and awareness, that can be ensured by access to information and its assimilation by users, which means that these two elements are conditional variables[13] for the independent variable. Thus, the intermediate variables represent conditions for the main variables (formulated in the primary hypothesis):

- The increase of the level of cyber security culture (independent variable) is

[11] Stephen Van Evera, *Guide to methods for students of political science* (Ithaca, New York: Cornell University Press, 1997), 9-13

[12] Ibid.

[13] Ibid.

ensured on the condition of developing cyber security education programs and awareness campaigns (conditional variables);

- ➢ Balancing the freedom / security ratio (intermediate variable) is ensured in the context of producing the effects of the independent variable - users know the threats and are aware of the need for security, these becoming conditional variables for the intermediate variable;
- ➢ The decrease of the cyber attacks number (dependent variable) is ensured in the context of the effects of the intermediate variable - the users apply the cyber security measures, also becoming a condition for the dependent variable.

In terms of phenomena, the proposed theory relates a specific explanation to the increase in the level of cyber security culture that can balance the freedom / security ratio, and the freedom / security ratio can generate a decrease in the number of cyber attacks. Thus, a high level of cybersecurity culture makes the internet user both a beneficiary and a provider of security, by applying cybersecurity measures in the online environment.

This thesis does not propose a philosophical analysis of the relationship freedom vs. security, but rather from a pragmatic perspective, which can be a model for adressing the way information is disseminated to users, either in cybersecurity education or in awareness-raising, in an attempt to formulate a series of answers to questions such as:

- ✓ What are and how can the threats, vulnerabilities and risks in the online environment be addressed, in order to ensure cyber security?
- ✓ What are and how can opportunities be exploited in the online environment?
- ✓ What are the common elements and where are there differences in cybersecurity legislation?
- ✓ What is the level of cyber security culture of internet users in Romania?
- ✓ Where is the balance point in the relationship freedom vs. security?
- ✓ Are freedom and security mutually exclusive concepts?

The paper, structured in three parts, addresses the issue of cyber security in three dimensions: the analysis of the evolution of cyber threats, the analysis of international and national cyber security legislation and, by applying an opinion poll on internet user behavior, assessing the level of security culture of users, as well as their perception of cybersecurity legislation.

The first part of the paper, Cybercrime, addresses threats, vulnerabilities and risks in the online environment, with an impact on society, at all levels, from the effects on simple users, to those that pose threats to national security. This section aims to analyze and define the relationship between the three concepts. For a better understanding of threats, the chapter presents the typology of cybercrime, from common cyber attacks, to cyber warfare, cyber espionage, cyber terrorism and hacktivism, as well as the tools most often used online by cyberattacks. Vulnerabilities, which are the key element in cybersecurity, and cybersecurity risks are presented in relation to threats. The chapter also includes a general assessment of the cyber security environment, focusing on recent transformations and future developments.

The main research method is the analysis of documents from various sources of information, such as papers and studies in the literature that address the topic of threats, vulnerabilities and risks in the online environment, both from a theoretical and practical perspective, in the case of those who analyze cyber attacks that have taken place over time.

For the theoretical notions, mainly primary sources were used, such as cyber security strategies as well as legislative documents or guides developed at the level of the European Union, or the North Atlantic Treaty Organization, through designated structures with responsibilities in the field, such as ENISA - Agency European Union for Cyber Security or CCDCOE - NATO Center of Excellence for Cyber Defense Cooperation. These were supplemented with information provided by institutions with a role in ensuring cyber security in the country and abroad.

There will always be threats in cyberspace, with a trend of diversification and numerical growth as technology develops. They must be known and evaluated and the optimal measures to stop their manifestation must be identified. Cyber security must be addressed on the basis of the characteristic of cyber threats to exploit the vulnerabilities of devices or networks connected to the Internet. The main objective of cyber security can be reducing the risk of materialization of cyber threats, which can be achieved by streamlining vulnerabilities management. However, there are always opportunities in this relationship. One of these, provided by the context, is that absolutely all stakeholders can act on vulnerabilities: users, authorities, developers of software and Internet connection devices, operators of critical infrastructure and digital services, international organizations, etc., and this will be possible when everyone involved understands that cyber security is a common responsibility, and each one will be aware of their own individual responsibility.

Most of the cyber attacks produced over time could have been avoided if minimal security measures had been ensured by users. From the most important, such as WannaCry, where the vulnerability was that the affected computers were running an outdated version of Windows, which no longer benefited from security updates[14]. In the case of Stuxnet, the virus was introduced into the system by connecting a USB to one of the computers. The cause of the success of most cyber attacks, however, is the opening of attachments or accessing infected links, received via email, messages or social media platforms, and the likelihood of their manifestation increases due to the absence of an antivirus program.

In the second part, using mainly the comparative method and content analysis, different legislative approaches regarding cyber security, national and international, both at the level of strategy and at the level of national regulation are studied, with the highlighting of some principles of international legislation, relevant in the field. Thus, in this chapter, the policies of the European Union and NATO regarding cyber security, the cyber security strategies of the member states of the two organizations, as well as their most relevant national cyber security laws are analyzed.

The chapter contains a section, dedicated to the evolution of the Romanian legislative framework, in the field of cyber security. In the end of it, there is a case study, consisting in the analysis of the evolution of the Big Brother law package, in Romania, as an attempt to identify the elements that were the basis of the failure of this legislative approach, as a reference element in the relationship between freedom and security, the context of national security.

Also, the paper aims to analyze and define the concepts of cybersecurity education and cybersecurity culture, as well as other specific concepts, representative in the process of ensuring

[14] Mikko Hypponen, „Mikko Hypponen speaks about WannaCry at SPIECES”, 2017, video disponibil la https://www.youtube.com/watch?v=ZqNSoHFtGM0, ultima accesare, iunie 2021

cybersecurity.

Cyber attacks depends on the negligence of users, employees or network administrators. Therefore, staff education, awareness and training, both in the public and private sectors, are aspects that cannot be ignored in the prevention of cyber attacks. Given that most of the vulnerabilities are generated by users, by accessing the Internet without minimum security measures, risks can be managed more effectively in the context of a high level of cybersecurity culture at society as a whole.

The impact of cyber attacks can be devastating in the private sector, but mostly in the public sector. In most cases, public sector targets are government or critical infrastructure. In both cases, the cost of recovering the systems after a major attack is huge, compared to the investment that any entity, whether public or private, can make in staff training and implementation of minimum security measures. Moreover, there are cyber security strategies in which the objectives, directions of action and related measures focus mainly on staff training.

Cyber security has three main components: prevention, intervention (reaction/ response), in the event of a cyber attack, and resilience, which are equally important and closely linked. Thus, preventive measures aim, on the one hand, to ensure the ability of systems to withstand cyber threats, and on the other hand, to reduce the impact of cyber attacks, through appropriate response measures, and thus the resilience of systems and networks is ensured by the efficiency both of the prevention measures and of the countermeasures/ intervention measures.

Primarily, prevention measures aim to ensure the resilience of computer systems and networks, which means that their effectiveness must ensure the complete elimination of cyber attacks. However, the rapid evolution of threats, capable of identifying and exploiting new vulnerabilities, requires the extension of prevention measures, in the sense of ensuring resilience by reducing the impact of possible cyber attacks.

While the prevention and resilience dimensions can be used mainly by specialists and those responsible, the prevention component, which consists of measures to reduce the risk of cyber attacks, is perhaps the most complex, given that all those involved, regardless of origin, level of use or level of training or specialization, they can contribute by respecting a minimum security protocol.

The first category of contributors is users (whether individuals, companies, institutions or organizations, as consumers of internet services), who must take protective measures, such as the use of passwords and an antivirus program, the careful selection of networks and of the sites, depending on the degree to which they present security elements, or attention to the content they post, distribute or access.

Another category is the private sector, with three major components - applications and devices developers, cybersecurity specialists - in principle, security software developers and security testers, but also operators and digital service providers. In the prevention phase, their contribution consists, to a large extent, in the provision of specific safe products and services, tested before being placed on the market.

The third category includes state authorities - the public sector, which has two subcategories, with different responsibilities. On the one hand, government authorities, as legislators, and on the other hand, institutions with responsibilities in the field of cyber security, established by law.

However, there are three other distinct categories, with an important role in the prevention component of cyber security, which cannot be assimilated to the above, namely: national essential service operators, which can come from both the public sector and from the private sector, and the CERT network, which has well-defined responsibilities, both in international law and at national level. In addition, at the level of each type of entity responsible for cyber security, there are cyber risk assessors, which form the CSIRT network and have a very important role in the incident response component, at the level of public sector institutions and at the level of private entities.

Each of the actors listed above may have obligations, but may also be beneficiaries of cyber security, based on a comprehensive law, which establishes exactly the role and responsibilities of each entity involved in this process.

Being part of national security, cyber security has proven to be a difficult area to legislate, but in the last two decades, there has been a major involvement of international organizations in regulating this area, or some of its components. NATO has defined and constantly updates its cyber defense policy, the European Union has issued directives and regulations, with obligations or recommendations for member states, regarding the drafting of national legislation, the OSCE and the United Nations have taken the first initiatives in this regard. These documents establish, adapt and define concepts such as sovereignty, jurisdiction or state responsibility, but an important aspect is the impact on human rights.

What is missing in international law is a treaty on the security of cyberspace, as it exists for outer space, air or sea, piracy or even Antarctic territory. But these treaties contain provisions on military action, so the models provided by these documents are not sufficient. Cyberspace is characterized by access to information and how it can be managed.

Regarding cybersecurity strategies, most countries in the world have developed such a document. The paper shows that all NATO and European Union member states have developed and implemented such a document. The problem that arises with regard to national cyber security strategies is that they regulate an area where developments are rapid, compared to difficult rule-making processes, and the needs of the state and society change with these developments. Cyber security requires a continuous and constant effort of the states. Thus, regardless of the content of the strategies, which at the time of issuance may fully meet the needs of a state, the national context must be periodically re-evaluated/ re-analyzed, simultaneously with the evaluation of strategy implementation, based on established performance indicators of developments, proactively. Today, some of the cyber security strategies of EU and NATO member states have been in place for more than seven years. Romania's cyber security strategy is one of these documents, being issued in 2013.

If at the strategic level, there are established visions, principles, objectives, directions of action and measures that respond to the cyber security needs of a state, depending on the analysis of the national context, at some point, the national law must establish the terms and method to implement the strategic provisions, with the establishment of responsibilities, attributions and obligations for all the entities involved, but it must also ensure the necessary measures and resources in fulfilling them.

Currently, in Romania, the field of cyber security is the object of the Cyber Security Strategy, from 2013 and of the Law on Cyber Security, adopted at the end of 2018.

The National Cyber Security Strategy is a comprehensive and coherent document, in accordance with the provisions of the European Union regulations in the field, for the period in which it was developed, but, compared to current developments in the environment it regulates, its provisions are largely exceeded, referring to the assessment of the security environment in 2013. The adoption of a new strategic document was assumed by Law 362/2018.

Law 362/2018 on ensuring a high common level of security of networks and information systems, generically called the Cyber Security Law, contains provisions regarding, in particular, the role and responsibilities of CERT-RO in preventing and combating cyber attacks, as well as the reporting of the other entities in relation to it. This law represents the transposition of the European Union's NIS Directive into national law and largely meets the requirements set out in the European document, but as the name implies. The law strictly concerns the protection of networks and information systems and provides for the establishment of the national authority in the field of cyber security, in CERT-RO and the CSIRT network, with tasks of prevention and response in case of cyber incident, as well as essential service operators and service providers. digital, in accordance with the list contained in the Annex to the document.

The most recent document referring to the field of cyber security in Romania is the Strategy for National Defense, which entered into force in July 2020. Although it is not a document dedicated to the field of cybersecurity, it emphasizes the approach to the concept of national security in a broad sense, including ”national defense - understood in two qualities, national defense and collective defense”, but also ”other dimensions such as foreign policy, public order, intelligence, counterintelligence and security, crisis management, education, culture, health, economic, demography, financial, environment, energy or cyber security, security of critical infrastructures and historical and cultural heritage” [15].

The document represents an important step in the evolution of legislation at national level, from at least two perspectives: it is based on an analysis of the current security context, revealed by the use of terms that were missing in previous documents, especially at the level of provisions on threats, and for this reason, it can play an important role in reviewing the National Cyber Security Strategy, but also in initiating steps to update national security legislation, as well as expanding cybersecurity legislation.

[15] Administrația Prezidențială, *Strategia Națională de Apărare a Țării pentru perioada 2020-2024. Împreună, pentru o Românie mai sigură și prosperă într-o lume marcată de noi provocări*, 2020, 7, https://www.presidency.ro/files/userfiles/Documente/Strategia_Nationala_de_Aparare_a_Tarii_2020_2024.pdf

From the analysis regarding the normative framework of Romania in the field, it results that a law on cyber security is needed. This should include in addition to the network security provisions of all institutions, especially those in the category of critical infrastructure/ essential services, by establishing and defining measures for: training staff on the operation of IT systems or the obligation to use antivirus programs, and the updating of software and, therefore, the inclusion of dedicated funds in the budget of the institutions concerned etc. Such a law must guarantee to the competent authorities, as they are called in the Strategy, the necessary tools in ensuring the component of the prevention of cyber attacks. However, prior to the drafting of the law, a new strategic document is needed, adapted to the current security environment, containing both tools for assessing the achievement of the objectives proposed in the previous edition and objectives, directions of action and measures to respond to new challenges of cyber security, established on the basis of an updated assessment of the security environment.

Another important aspect in ensuring cyber security is cooperation, both at international and national level. If, at international level, cooperation is guaranteed by membership or ally status in international organizations, at national level it consists precisely in the relationship between the public and private sectors, and a component of it is the relationship between authorities and the owners of communications networks. This relationship can take place in three dimensions. A first aspect is to ensure communication between entities, provided by Law 362/2018 which establishes CERT-RO as ”competent authority at national level for the security of networks and information systems”, with responsibilities in collecting notifications regarding cyber security incidents, such as and the establishment of the CSIRT network. The other two dimensions must be ensured by subsequent provisions: on one hand, by implementing measures relating to the certification of IT products, services and processes, in order to reduce vulnerabilities related to internet connection and, implicitly, to protect users, and on the other hand, by ensuring measures and instruments to achieve national security.

Staff training, education, awareness campaigns and security culture are provided for in the 2013 Strategy, but they are not covered by the current law on cyber security. If staff training and cyber security education need legal provisions to implement measures accordingly, information and awareness campaigns at the user level can be carried out without a dedicated law. These are all the more important at the level of the Romanian society, as it is necessary that the adoption of laws that respond to the security needs, including from the perspective of national security.

Given these data and related to the background of national security laws, in force for almost 30 years, which are adapted to the threats at the time of their issuance, the measures to ensure national security are limited. Therefore, Romania needs a complex and coherent cyber security law that meets the protection needs of all users in the cyber environment, especially since today, there are very few activities that do not take place online or are not connected, at least partially, to it, but also to the needs to define and update, in the context of the technological era, the capacity of action of the authorities with attributions in the field of national security.

Currently, the legislation establishes the institutions with responsibilities in the field, the system and the way of working within the CSIRT network, which is composed of such centers in all key areas, establishes the list of essential services and that of digital service operators, as well as the coordination and liaison with CERT-RO, as well as the designated national authority and single point of contact in cyber security field, thus meeting the strategic objective of critical infrastructure protection. The objective is to monitor cyber threats to Romanian infrastructures and protect them accordingly. It can be said that, thus, the communication platform was created, described in the paper as situational awareness, which allows, through direct coordination and collaboration, the shortening of reaction times in case of a cyber crisis.

Moreover, according to the statements of the director of the National Cyberint Center, Anton Rog, during the Security Talks conference[16], in the next period, CERT-RO will become the National Directorate for Cyber Security (DNSC), which will act as a ”hub between all enforcement institutions of law, intelligence, military and private industry, and academia”, which will ensure its status as an ”institution (...) of international level and a key player for the implementation of the national cyber security strategy. (...) The directorate should be able to firmly position Romania as a recognized leader in cyber security”[17].

[16] Security Talks Expert, Security Talks Conference #3, 2020, https://www.youtube.com/watch?v=0nH9TrhenEs, last accessed, November 2020

[17] CERT-RO, „Ce va aduce nou Directoratul Național de Securitate Cibernetică față de CERT-RO”, 2020, https://cert.ro/citeste/articol-dnsc-cert-ro-transformare, last accessed, November 2020

Therefore, DNSC is the platform that can integrate solutions to meet the objectives of internal cooperation, both between institutions with responsibilities in the field of cybersecurity, and between public and private sectors, but also those of international cooperation, by positioning Romania as a leader in in the field of cyber security, in support of which it is relevant the establishment of the European Center of Competence in Cyber Security in Bucharest[18]. The activity of this European center will focus on ”innovation and research and development in the field of cyber security” projects[19].

However, it remains a challenge in developing and implementing measures to increase the level of cyber security culture of citizens and, in particular, the security culture, necessary in balancing the relationship between security and freedom. As the opinion poll, detailed in Chapter III, pointed out, there is a need for better information on the cyber security measures that users can take.

Many of the cyber attacks can be avoided if there is a coherent regulatory framework, comprehensive and adapted to the evolutions of the environment it regulates. For example: the cyber attack on four hospitals in Romania, in June 2019. According to the authorities, it was a ransomware attack, activated by accessing an e-mail attachment by hospital staff, in the context of the absence of an antivirus program. Therefore, this attack could have been avoided if, on the basis of obligations established by law, hospital staff had been trained on minimum protection measures in the online environment, on the one hand, but also the provision of the necessary resources, on the other. The incident could have had much more serious effects, given that hospitals were targeted - constituent elements of the health system, included in the category of national critical infrastructures.

Finally, in the third part, the method used is the opinion poll, consisting in the application, in the online environment, of a questionnaire on the behavior of internet users, which balances, on one hand, the way in which they they try to protect themselves in cyberspace, and on the other hand, their perception of regulation in the field. This tool can provide both the

[18] Consiliul Uniunii Europene, „Noul centru de competențe european în materie de securitate cibernetică va avea sediul la București, România”, 2020, https://www.consilium.europa.eu/ro/press/press-releases/2020/12/10/the-new-european-cybersecurity-competence-centre-to-be-located-in-bucharest-romania/, last accessed, June 2021

[19] Security Talks Expert, Security Talks Conference #3, 2020

elements necessary to assess the level of cybersecurity culture at the level of users, and those necessary to identify exactly the balance between the concepts of freedom and security, defined by the extent to which they can accept a regulation, which can be perceived as limiting or even intrusive in the field.

In conducting the opinion poll, four categories of questions were established, grouped into four sections:

- ✓ Introductory questions;
- ✓ Questions regarding the behavior of users in the online environment, as well as the security measures they use;
- ✓ Questions regarding the opinion of the respondents on the possible threats and protection measures that can be applied in the online environment;
- ✓ Questions regarding the respondents' opinion on the events in reality, aiming at the protection of personal data, the use of technology by the authorities in certain situations or a cyber attack produced in Romania.

The survey was applied on the www.survio.com platform, and SPSS software was used to interpret the survey results.

The research method using the survey has a number of limitations, which generally stem from the fact that it will be applied online. It gives it a voluntary character, which can directly influence the achievement of a representative number of subjects, on the one hand, and the fairness of the representativeness of the target audience (internet users), depending on criteria such as: age, sex, education, income or background, on the other hand.

Also, the period of time in which such an instrument can be operated is directly influenced, as the distribution routes are exhausted in the first days after activation, and the degree of redistribution decreases proportionally, related to the time elapsed since the launch. Therefore, the survey can outline a robot portrait of the internet user in Romania, but the results can be extrapolated to society only if a minimum sample of respondents is reached.

The research on assessing the security measures that users take in online activity, the extent to which they can identify possible causes of cyber threats or possible solutions, and the perception of cyber threats and responsibilities or who they belong to, revealed an average level of users' cyber security culture, but with development potential, given the identification of users' need for better information, and a low level of security culture, which reflects an imbalance in the freedom-security relationship, in favor of freedom. Security measures associated with the intervention of the authorities are an option for users, only conditionally. There is a relatively low level of acceptance of legislation in the field of cyber security and reluctance on the measures to be taken by the competent authorities in the field of national security, but the respondents are open to their actions or attributions, conditioned by the knowledge of the phenomena, for which the solution is precisely to inform the users.

This imbalance is based on the lack of information and creates a dangerous background, in relation to the legislation of some aspects related to national security: most of those who oppose regulations in the field, are those who can opt for security, in the context of a major crisis, as was the case with the adoption of the Patriot Act in the United States.

In the context of the debate on freedom vs. security, the perception of the two concepts is that security measures affect the rights and freedoms of citizens, especially from the perspective of ensuring national security. However, in a democratic state, security can be ensured, while respecting human rights, as „the citizen participates in ensuring security" [20].

The average level of cybersecurity culture compared to a low level of security culture are caused by the lack of availability of information in the field. Cyber security education, as well as awareness-raising and staff training campaigns in public and private organizations, can be equally responsive to such needs. Unlike the field of national security, where information for citizens is quite limited and thus they are only beneficiaries of security, on the component of cyber security, they are directly involved, being users of this space, which makes them equally security beneficiaries and providers, through the measures they need to take for their own security. If this information, made available to users in the context of cyber security, also covers the responsibilities of national security authorities, so that security measures can be understood through the filter of the online environmental user: the existence of threats, the need for

[20] Monitorul Apărării și Securității, Sergiu Medar, at the Conference *Cum răspundem la crizele de securitate națională*?, 2021, video available https://www.facebook.com/monitorulapararii/videos/1136156286802705/?__so__=permalink&__rv__=related_videos, last accessed, February 2021

protection against them, by understanding the effects that can have and the importance of implementing security measures, at the level of critical infrastructure, the level of security culture of a society can be increased through information activities dedicated to cyber security.

By education and awareness, users can learn the threats and vulnerabilities, as well as the effects that possible cyber attacks can have on them, and also, being aware of the need for security, they will use the methods and means thay can use to ensure protection against them and they will know who to turn to in case a cyber security incident is identified. Knowing the legislation is another key element that can be the subject of cyber security education and awareness campaigns. In addition, users can learn about the institutional architecture with responsibilities for ensuring cybersecurity and how these structures work in ensuring cybersecurity.

If awareness can be made through information campaigns, aimed at the general public, with the sole purpose of raising users' awareness of cyber threats, as well as the means of ensuring security in the online environment, the education component refers to educational programs included in the school curriculum, depending on age, from primary school to high school. At university level, the specialization component can be developed. Thus, the benefits of cybersecurity education can take new forms: on the one hand, better trained users will be prepared to face online challenges, and on the other hand, deepening this field in academia can provide cybersecurity specialists, a human resource that can operate in both the public and private sectors, both in the area of policies development in the field and their implementation. Another benefit of cyber security education can be the research and development field, by involving specialists trained in such an educational system in the development of communications products and services and information technology at higher security standards.

Staff training represents another way to inform users in cybersecurity. Training programs are needed for both public and private staff, especially in the case of entities active in providing essential services.

All these methods of informing and training users, specialists and human resources, consist in providing relevant cybersecurity information, including the legislative dimension, which defines responsibilities for the authorities with responsibilities in the field, and the result of these information measures, cumulated, consists in obtaining a high level of cybersecurity culture at the level of society.

The main result of such an approach is a balanced relationship between freedom and security, by understanding the concepts of responsibility, both individually and collectively. This is the stage in which an online user behavior can be outlined, adapted to the challenges of the cyber environment, which consists in the permanent application of individual cyber security measures. This behavior is based on the awareness, equally, of the need for security and freedom, by users, so that they are not mutually exclusive, but rather can be complemented.

The immediate consequence of such behavior is a decrease in the success rate of cyber attacks, which is the purpose of cyber security measures.

Related to the topic of freedom vs. security in the online environment, other research directions can be followed. For example, the paper proposes to prioritize actions to increase the level of security culture, which depends on the development of awareness programs throughout society. Also, the thesis provides a model of structurating the message within an awareness campaign for users, who understand that they need to protect themselves in the online environment, through information on threats (why protect themselves) and cyber security (how to protect). Subsequently, using the process tracing method[21], there can be made the evolution and impact assesments regarding the level of security culture increasing measures, through education and awareness, or in an analysis dedicated exclusively to this evolution, can be evaluated, in stages or in relation to the level of acceptance of the implementation of some legislative provisions regarding the national security, the freedom-security ratio being specific to this field. The survey presented in the paper can also be an assessment tool, which can be used both by independent researchers and at the level of the authorities, when reviewing strategic documents on cybersecurity. Their updating is necessary from the perspective of the permanent evolution of threats, influenced, in turn, by technological development.

[21] Stephen Van Evera, *Guide to methods for students of political science* (Ithaca, New York: Cornell University Press, 1997), 64