BABEȘ-BOLYAI UNIVERSITY
FACULTY OF HISTORY AND PHILOSOPHY
„*INTERNATIONAL RELATIONS AND SECURITY STUDIES*” DOCTORAL SCHOOL

THE NATIONAL SECURITY GOVERNANCE: THE SECURITY MANAGEMENT OF CYBER SPACE, BETWEEN REALISM AND SUPRANATIONALISM

****

PhD THESIS SUMMARY

Scientific adviser:
Prof. univ. dr. ADRIAN-LIVIU IVAN

PhD student
George-Marius ȘINCA

Cluj-Napoca
2021

TABLE OF CONTENTS

KEYWORDS:

CYBERSECURITY CULTURE, REALISM AND SUPRANATIONALISM, CYBERSECURITY GOVERNANCE, CYBER DIPLOMACY, CYBER RESILIENCE, GOOD CYBER GOVERNANCE

In the current context of global security, the outcomes of globalization, the recent geostrategic, geopolitical contexts as well as those of the alteration or hybridization of financial and economic mechanisms -*which represent the results of information explosion and technological hyper development in the field of information and communications technology*-, new paradigms emerge that often overturn theories or change the progressive trajectory of reference fields such as economic, political science *(national and international)* and international relations. Therefore, new sub-domains are developing in the diplomatic sector *(digital diplomacy and cyber diplomacy)* that change the paradigm of national and international security - with these changes, elements appear that lead to a reconceptualization of the intelligence sector. Consequently, we are witnessing a natural transformation of all existing and connected cyber domains in all sectors of contemporary society.

This global paradigm generates a complex international dynamic that requires a permanent analysis of the effects recorded at international, supranational and national level. Commencing from this phenomenon and completing conclusive case examples such as the constituent elements of national cybersecurity incidents - *Estonia*[1] *(2007)* – and of course, the signals of cyberattacks increasingly targeting the private or government sector in Europe and other states offensively or defensively, I sought to identify the measures and countermeasures taken by states, federations or unions to limit these attacks and to get a crystal view on the need to ensure a degree of resilience appropriate to the degree of risk associated with each case..

The present paper presents itself as an exploratory and not necessarily exhaustive perspective on the protection matter of national resources and values in the spirit of the supranational concept. A second element that brought my attention during the period allocated to the analysis of cyber attacks was the vulnerability factor given the lack of a culture of security of the entire population and security culture illiterateness in the cyber environment, both among the decision-makers and the general diplomatic sector.

The overall objective of the thesis is to investigate the relationship between elements such as national security governance, resilience, diplomacy, jurisdiction and good governance of the cyberspace to confirm or deny the typologies and new information systems in the virtual space as well as their contribution to the virtual governance balance between realism and supranationalism.

Specifically, three secondary research objectives were formulated to *identify the interdependence between cyber sector governance and national security, to identify the determinants of national security governance resulting from adapting the information security management system in the virtual space and to study the paradigm of information security governance in the virtual space in the consent of realism and supranationalism.*

The purpose of the scientific activities carried out during the documentation period and in the conceptualization and writing phase of the paper, was to identify and treat a new approach to ensuring national security by creating logical and interdependent connections and relationships between concepts

[1] Rain Ottis, CCDCOE, „*Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective*", Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, 2018, https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf, accesat astăzi 20.12.2019.

such as: *the organization, information management, cyber area, supranationalism / realism, diplomacy, cybersecurity culture and national security.*

The general hypothesis of the research appears to achieve the proposed objectives, where it was considered that good governance in the cyberspace can contribute to solving the security paradigm and dilemma in this new area. By theorizing through the resources of the scientific research methods addressed and applied, I will be able to highlight whether there is an interdependence relationship between the practices of governing national security systems and the supranational systems and the relationships between them. The working hypothesis was tested through a case study, in the last chapter of the Thesis.

The research methodology underlying the concept of this paper is one based on the inductive study of the national, European and international legislative package on cybersecurity and the study of the specialized literature confirmed by the exhaustive results of the case study on the cybersecurity culture of the resident population from Romania. Founded in the existence of the general-specific "research binomial" applied throughout the paper, it has proposed generating general conclusions regarding the governance of national security by demystifying the management of virtual space security in the perspective of realism and supranationalism. Methodologically, the preliminary conclusions of the first five chapters together with the entire chapter six, are the result of a scrupulous analysis. Among the main methods of data analysis and evaluation of the research variables was *the method of competing hypotheses (used in the simplified variant of inconsistency assessment of hypotheses). The method of the case study* in the present paper is built using the cross-checking methods, to test and experimentally verify the theoretical-applicative value of the research results obtained from the research of the proposed topic. In the present paper, the case study is related to a final sample of 5,446 persons out of the total of ~ 7,600 questionnaires applied, which represents ~ 0.03% of the 19,644,3501 persons, which is the estimated number of the resident population in Romania for 2017.

For reasons of academic equidistance and balance, we considered the following fundamental research principles:

- *the principle of exploration and description of phenomena* - the paper focused on an exploratory study namely on the description and exploration of the relations between phenomena;
- *the correspondence principle* - the results were based on a permanent connection to the contemporary academic and scientific knowledge;
- *the principle of observability* - during the paper rationally presented arguments that can be verified at least at the cognitive level.
    - *conducting interviews* based on the results of the questionnaires obtained during the research;
    - *consulting* with practitioners in the field or related fields - in a formal and informal framework;
    - *studying primary, secondary and tertiary documents;*

The most important tools for working in the scientific research process were the following:

- The Brain, R, IBM SPSS Statistics for Windows, ACH 2.05, IBM i2 Analyst's Notebook, MsOffice 365;

- Mendeley, O'Reilly, Safari, Archive.org, Statista, Klarmedia, IEEE Xplore Digital Library.

The thesis is divided into two main parts, sequentially into six chapters. The first part is composed of the argument of the paper, which represents, of course, an empirical perspective on the content and which briefly sets out the information from the organizational perspective that will be later analyzed in the first chapter in an inductive and introspective way. In the first five chapters, all references to information are finally oriented to its approach and its effects, in its digital form in a contemporary security context. The second part is represented by the fifth chapter, which is the last one, where the relationship between the security culture of the individual who is at the same time the end-user connected in the cyber area is demonstrated, with the security in all its forms, specifically listed, human security and cybersecurity as a sub-domain of national security. It is worth mentioning that the sources that generate insecurity, such as communities or digital societies that do not have the knowledge or a general culture of security, are without a doubt a negative factor brought to the concept of national security. Of course, the last chapter becomes by extrapolation a new field of study for the author and an academic research for the scientific community, but it is not, however, treated as a separate study, which is rather focused on obtaining quantitative and qualitative data to substantiate and validate or to invalidate the research hypotheses from the first part of the paper. Being an exploratory research, along the scientific path and based on a positive critical spirit, remarks were made regarding the dynamic character of the paper, considering that the research goes from general to specific and contextual from specific to general but which in final results in an objective positioning of conclusions on the chosen topic. Each chapter has sections and subsections and presents elements that contribute to the testing of our research hypothesis.

NATIONAL SECURITY GOVERNANCE:
VIRTUAL SPACE SECURITY MANAGEMENT - WITHIN REALISM AND SUPRANATIONALISM

CHAPTER I
INTRODUCTION

Naturally, based on the author's experience in the field, an absolute need to research the new sectors of cybersecurity and governance has been identified. These areas represent a priority area of research and innovation for Romania and the EU. From the perspective of the sustainable development of cyberspace, a lack of cybersecurity research is identified, in the context of international relations. The number of Romanian researchers dedicated to the study and developing specific solutions in the field of international relations, security and studies in the cyber domain, which leads to a decrease in the capacity of the Romanian contemporary defense and security system as well as to a deprivation of the strategic security resources, much needed today for a country with considerable Euro-Atlantic ambitions at least in the field of cybersecurity and for a short time at the helm of the European Union.

An objective list of the factors that led to the selection of this study is given not least by the assumption of security and governance of the European cyberspace identified as a priority topic on the agenda of the European and international community, where the scientific achievements of the Romanian authors are generally relatively low, hence, the author was forced to study and analyze the works of the authors established in this field from the international scene. A limiting factor, self-imposed, regarding the study and citation of sources was given by the desire to separate the arguments pertaining to the sciences of international relations and the security studies to the arguments of law and jurisprudence brought by the legal sciences of national and international law. The reason for this choice was given by the need to report and concentrate the research process on the author's field of study, namely that of international relations and European studies.

The concept of "national security". Over the years, in the context of different areas of research, within the numerous scientific circles, theoretical debates have been a common topic more or less substantiated in concrete. The concept of security still retains its ambiguous character but which, in the process of researching international relations, is often used as a pretext, excuse or justification for the various objectives or political or strategic results. As for the definition of the term "national security", it often suffers reinterpretations given by the interpretation in the spirit of the law of a set of official documents that are updated annually or at a frequency of five years - here referring directly to national or sectoral strategies in the field of defense, national security, priority plans issued by CSAT or C.N.I.

During the documentation and even before the research process itself, the question arose whether the assessment of the cybersecurity level of the population reflects a sufficiently large extent of any aspect of national security. Considering that, the presumption of innocence and the human factor - of confidence - was at the base of the design and consolidation of the cyberspace, this evaluation is necessary. One of the former presidential advisers on national security issues stated the following, *"in national security policy you have to manage those developments, those problems that can quickly generate national security crises, which in days or even hours, endanger your territorial integrity, sovereignty, the safety of a large number of people. "* - From this statement strongly based on facts, political actions and European history we understand that the cyber area is extremely important in ensuring a high degree of national security.

CHAPTER II
MANAGEMENT OF THE INFORMATION CIRCULATED DIGITALLY

In the context of the thesis, **information management** is the result of *managing the relationship between the identification of vital information - centralization - analysis and synthesis to classify furthermore use it for delivery to the decision-maker moreover to use it efficiently.* Considering that the degree of performance of the governance of an environment, even of the virtual one, relates to the quality, the veracity and the moment of the information delivery - so we can say at the center of the information systems governance and of the entire cyber area lies the information. Whether we are talking about the military, government or civil sector, no matter what purpose is used, the information takes on a tactical and operational attribute considerably.

The information, in any form it would be necessary to be identified, observed, extracted, analyzed and processed to be able to assign a value for its use, which is why the relevance of information management in electronic media in the context of the analysis field of security studies it is a vital one for both the beneficiary and the corporate, industrial, governmental, political, diplomatic, senior governors or any state or non-state actors whose decisions revolve around this information.

The need for a well-structured **information system** is felt in organizations where information is not only sensitive, its dynamic attribute makes information that is not in electronic format more difficult to duplicate, manage or archive; on the other hand, their alteration is, in any case, inevitable while a document in electronic format (text, audio, video) managed according to the minimum security rules is not as vulnerable to these risks. However, it should be mentioned that the volume of information increases exponentially and with the technological progress, population growth and sources of information generation, therefore the information has a different rhythm of generation, propagation and dissemination, which is why we must pay greater attention to its verification without you reach the uniqueness and the generating factor.

The questions from which the answers will result in possible solutions to the current situations of the contemporary organizational system regarding information management are the following:

- *What does the organization represent from an informational point of view?*
- *From the perspective of risk management, the vulnerabilities, the risk variables and the implications to which information systems are subjected to and within the organization?*
- *Is the need for a reorganization of security and information management in an organization something that we should pay attention to?*

The organization represents a dominant entity in all sectors of society, as a form by which the collective energy is combined with the aggregated individual skills, for the achievement of most categories of economic goods. Thus posed the question of definition, it can be stated that *"an organization is a group of people who act in a correlated way to reach a common goal".* In the context of the sustainability and governance of the management system, we find ourselves in a dynamic sector, sensitive to changes, contextually some organizations appear, others disappear, some merge, others diminish their weight while others grow rapidly, and others struggle to survive. Virtual organizations have emerged that are set up in the form of fast communication networks mediated by new IT technologies. But even so, due to the diversity-generating sources, the survival time of an organization in shape, size and profile has been reduced considerably, after some estimates at 5-10 years.

The character of the information should be treated according to its dependence on the **temporary factor** such as: *planning, actuality, frequency and time of time in the form of the information as well as the clarity,* *granularity, sequentiality, the mode of presentation and the support on which the information can be delivered.* In terms of **content**, information should be noted for *accuracy, relevance, completeness: brevity, objectivity and performance.*

The value of information, data, as well as the costs and benefits resulting from its processing become more and more transnational. The information represents in any field of activity - *academic, research, innovation, industry, local or central administration, government, legislative, national security, etc.* - an undeniable resource of high decision-making power, often of unquestionable and invaluable value, often supplemented by storage and processing systems that can provide a certain advantage in managing sensitive events or closed or open conflicts.

From the analysis of **risk management in contemporary organizations** in relation to the resident population in Romania and active in the field of work, we can observe a lack of cybersecurity culture, which is why security incidents and cybercrimes are so common and have such a great impact on both individuals and organizations. Continuous training on the specifics of information protection and defense against risk factors is undoubtedly one of the first needs of the organization. The quality and existence of a community of information security elites in any organization are imperatively needed to cover the second fundamental level of human need, particularly security, which is nowadays largely represented by the cyber area. The creation of inter-human relations through communication, consultation and collaboration between the management and the execution area in the organization increases the confidence level of the security system. Failure to meet the primary logistics needs of the security system (*equipment, audit, management, research, security studies experts and security engineers*) leads to an information collapse. Due to the ongoing evolutions of the cyber world for better governance, a permanent updating of the national and international legal framework is needed.

Based on the need for the good governance of the information system and especially of the information, to obtain the most effective and good decision - especially in the context of national security - we observe that there is no room for error, even from the government sector. And yet whether we are talking about so many nations, federations, unions or other supranational forms, we must take into account that any state needs to be sovereign or sovereign within the alliance. The primary resource with which it is working, for the moment, is the human resource, which is why the information can be slightly altered (directly or indirectly). Due to the limitations of the human resource, due to the lack of human processing capacity, new intelligent processing systems have been developed - we find in this sphere of interest and research:

- automatisms and mechanisms based on artificial intelligence with extraordinary processing capabilities, which has no human reason and emotion;
- machine-learning systems based on previous processes (success/failure) called artificial intelligence and its sub-dimensions such as the concept of "machine learning" or "deep learning";
- systems established with the help of which functions of processing and prediction can obtain the best results for the management and the organizational progress, which each time is quantified in financial resources.

Security policies take different forms, depending on the "*good*" that needs to be secured, its actual value, the "*purchasing power*", the owner and the beneficiary of the information, the interests and the effects of its dissemination in certain areas of interest, mentioning that the effects are usually measured in economic, financial or power dimensions.

The novelty elements presented in this chapter are given by exposing the need to conceptualize a new framework for analyzing and governing material and cyber resources for good governance of the cyberspace with the help of the elites formed in the newly created niche sectors. To reinforce this vision, I consider the theory of changing primarily applicable in the area of international relations research related to this new virtual area emerged and whose effects in the area of governance of the information sector cannot be ignored.

The theory of change is a key element in the progress of all sciences, which is why it must be adapted to the new contemporary digital information context. Theory of change and the cybernetic area are two of the most important elements of the new era - whether it is quantum or something more.

International relations is one of the areas in which Theory of change is applied in two forms, namely in a controlled form based on interdependencies or in an imposed form, either supranational or based on the international or global context.

In this sense, it is confirmed that good governance is based on the applicability of the theory of change in a supranational context with the preservation of state sovereignty and alignment with the group vision. This theory even defines the balance of *realism - supranationalism.*

CHAPTER III
THE GOVERNMENT OF VIRTUAL SPACE IN THE CONCEPT OF REALISM AND SUPRANATIONALISM

In the current geopolitical and international security context, influenced by the cyber area that lacks tangible borders, political realism acquires a completely different definition - the paradigm of realism is partially changed. However, to be cautious about claims of such magnitude, I believe that an interpretation of realism is needed, taking into account the influences of the progress and innovation of contemporary technology and the cybersecurity paradigm in the context of the national and federal government or even global.

In order to be able to analyze realism in the context of the governance of international relations, there is a need to understand the concept of realism as a defining term for the theory that supports it. Therefore, knowing that international relations also represent the inductive study of the interactions and reports of state actors to non-state actors, we consider political realism as one of the main theories that try to explain the relations between them, that is between states. In an attempt to explain the international relations between states in terms of power, political realism brings forth concrete and adapted arguments on the capacity of self-governing states.

Important terms in the context of realism

In the context of international relations, the term power is, in principle, represented by the ability of one state to convince another state in making decisions that it would not normally or naturally take or the power of a state to stop internal or external actions of another state, actions that it naturally wants to exercise. A defining aspect, in this case, is the "imposed" power of some states on the decisions of other states irrespective of the influence and internal pressure of the state on which the international political power manifests itself.

The assumptions of realism

We want an understanding of the mechanism of governing the cyberspace from the perspective of national security through the concept of realism and supranationalism. Following the hypotheses listed above, some correlations can be identified between the type of EU governance concerning the Member States and with non-member but partner states. At the same time, it is very easy to see how states are struggling to maintain a balance between maintaining their sovereignty in federal construction and at the same time trying to align themselves with the common goals and vision.

For example, in the context of realism and liberalism, sovereignty can be defined by the quality of the main attribute of the state where, this implies the idea of territory, population and an efficient government and of course, if we consider the three constituent elements of the state, it can be observed that this definition is unanimously applied by all 193 member states within the UN. Currently, two interpretations of sovereignty are disputed, namely state sovereignty and national sovereignty.

Balance of powers

Taking as an example sports performers who possess physical qualities that most people do not have or by observing the intellectual resources that geniuses have, we can understand why not all countries have the natural capacity to become strong enough to stand on their own or to stand on their own to impose in the international relations sector.

And in the international relations sector, there are states or non-state actors that bring potential risks to the national security or to the integrity of the alliances in the international arena, they rely almost every time on highlighting the ratio of forces and implications brought about by their value on the international relations "*market*".

Under these conditions, a state that does not have the resources to oppose it can appeal, according to the supporters of the current of realism, to the principle of balance of powers. This brings to the fore the possibility of empowering the resources of one or more states to balance the power of one or more states to harmonize a state of equilibrium.

Cyber power in the context of contemporary realism

Power is a defining element, essential even for realism, because it can ensure the independence and survival of the state in a self-governed and self-sufficient environment. As Morgenthau states *"whatever the ultimate goal of international politics, power is always the immediate goal"*[2]. Often the supporters of realism relate power with an essential state resource such as natural resources, industrial capacity, military strength and the population of a state. Cyber power is defined by Nye as "the ability to achieve discounted results by using the resources of interconnected information systems in the cyber sector", and the potential of this kind of power to transform or redefine conceptually but also international relations has become a prominent debate in the field at a global level. Although we can see, the absence of a theory on cyber power in the realist literature does not stop the realism in developing a broad study framework in which to generate various hypotheses of power distribution between state and non-state actors in the virtual sector as well as in the way which is dealing with cyber conflict from the perspective of realism.

Neorealism and the distribution of power

Like many other theories, realism has evolved. Neorealism, also called structural realism, focuses more on the structure and distribution of power in the international system than on the power characteristics of individually perceived states. A key concept in neorealism is that of polarity, which describes the power structure of the international system. You can think of a pole as a state that is a center of power that attracts others in its sphere of influence, just as the pole of a magnet attracts metal casting or the gravity of the sun draws the planets into orbit around it.

One of the long-term debates was that of a possible multipolar, bipolar or unipolar power configuration to find its balance and management in creating a more peaceful world.[3]

The distribution of such capacities between states is considered to have significant implications for the stability of the international system, especially from the perspective of national security.

Applied realism: cybersecurity

Realism has long been and still is a dominant paradigm in the system of international relations, well defined but in some dilemma regarding the cybersecurity sector that is developing. This new area presents a revival of the perspectives influenced by realism, with a visible focus on security and competition, on the redistribution of power, on the advantage of the offensive on the defense and the benefits of the deterrent strategies, thus offering an opportunity to evaluate the role of realism in these unspoken debates[4].

The theory of realism, having as a general concern, the issue of security and the factor of national power, seems to be one of the preferred perspectives and tools in the process of analysis on understanding conflicts in the cyber sector in the context of international relations. Realism remains a relevant framework for

[2] Morgenthau Hans J., "*Politics among Nations: The Struggle for Power and Peace*", 1949, New York, Ed. Alfred A. Knopf, p.13, https://archive.org/details/in.ernet.dli.2015.74487/page/n35, accesat astăzi 29.11.2018.

[3] Mearsheimer John Joseph, International Relations Theories: *Discipline and Diversity, "Structural Realism"*. revizuit de Tim Dunne, Milja Kurki, Steve Smith, Oxford, Anglia, 2006, Ed. Oxford University Press, pp.71–88.

[4] Anthony J.S. Craig, Brandon Valeriano, „*Realism and Cyber Conflict: Security in the Digital Age*",Ed. E-International Relations Publishing, Bristol, Anglia, 2018, p.86.

identifying important cybersecurity issues and can sometimes provide useful insights into some of the features of international relations. However, realistic conflict theories are often not sufficiently relevant in explaining the unique dynamics of cyber conflict or in creating an objective conflict forecast.

Cyber weapons race as a result of contemporary realism

As for the reports in the media about a possible cyber weapons race, these are becoming more frequent, and this tendency of militarization of states in the cyber space is obvious. Clear signs of arming are also the emergence of new military organizations or forms of military organization in the state armies, the elaboration of cyber doctrines and strategies in the military sector, the increase of budgets in the sector of cybersecurity development and innovation, as well as the engagement of cyber "*warriors*". We can create an overview of the development area in the cyber sector only regarding malicious programs such as "*Stuxnet*", which was developed in the highest secret and used exactly in the idea of reaching the realistic goals of a country regarding another state. which was a global insecurity generator. We can say that this new type of "*product*", although intangible, extremely dangerous, the cyber weapon can enter the military arsenal of a country. Besides, a significant number of specialists, journalists, observers, or state security reports provide empirical evidence that demonstrates an interrelated relationship between cyber sector development and other states' perceptions of a possible cyber threat as well as generating a competitive spirit between states[5].

Analysis of the cyber (in)security spiral in a contemporary context

At this moment there are more or less diplomatic discussions that have as their main purpose the nuclear disarmament, coming precisely from objective reasons supported by the realistic ideology of the states, with results less favorable in the global interest and favorable to the few. The question that naturally arises is about the existence or modality of digital disarmament of a country.

In this hypothetical context, of the need for digital disarmament of a nation state, what are the implications and what is the size of the collateral damage brought not only to the government sector but also to the civil sector. If the size of a country's nuclear disarmament is military in nature and unlikely to directly affect the civilian sector or the public-private sector, in the context of a digital incapacity or disarmament, the symptoms will be felt in the inverse relationship among the population.

Theorizing the offensive-defensive balance in the cyber sector

When the advantage lies with the attackers, the great powers are strongly challenged to increase their offensive capabilities and to seek ways of territorial expansion or power through new strategic alliances to consolidate their position, otherwise, they risk to identify in a defensive position what is not desirable because the pressure and risk of being attacked is imminent. It is considered that the factors given by the technological evolution define the defense-efficiency balance and offer new perspectives. For example, it is said that technologies to improve mobility in the five major areas (*terrestrial, maritime, air, cyber and cosmic*) favor attackers, while technologies that increase and optimize firepower strengthen the defense sector, making it more durable and efficient. The theory has been applied to define the possible onset of conflicts or the absence of wars during history.

The theory of offensive-defensive balance has been completely reconceptualized due to the emergence of this new area where the applicability of this theory was possible. The reconceptualization was due, in particular, to the non-territorial nature of the versatile and binary code-based cyber technologies to the

[5] Anthony Craig, Brandon Valeriano, „*Conceptualising cyber arms races*", *8th International Conference on Cyber Conflict (CyCon),* Ed. NATO CCD COE Publication, Tallin, 2016, https://www.researchgate.net/publication/305871947_Conceptualising_cyber_arms_races, accesat astăzi 06.12.2018.

detriment of fire ammunition, which strongly replaces the need for mobility and firearms capability in the other four real spaces.

Supranationalism

Understanding the supranational term as an ideology opposed to realism is, in my view, an erroneous and devoid of rational foundation. Supranational bodies are given greater powers and authority over certain aspects of the union and the member states of these unions, but we must not omit the purpose and goals for which these states joined these unions. „*Through their forces, the states certainly could not deal with certain problems or even more so they could not effectively manage or manage them under the progressive conditions of the unions such as the European Union or the desired model of the United States of America. In the case of Romania which has the status of a member country of the European Union, we can say that the strategy and the process of European construction are based or even begins with the strengthening of national sovereignty. Whatever the case, the national project cannot under any circumstances be opposed to the European project"*[6].

If we do a brief analysis of the EU, starting from the previous premises, we can say that it is a supranational organization that has con-federalist elements (treaties, a Council of Ministers, which has legislative and decision-making powers, the Council, the main political authority, the rule unanimity in the decision-making process) the federal ones (common citizenship, single currency, the primacy of Union law vis-à-vis the law of the Member States, supranational institutions, etc.).

To become a federal state, the European Union needs a Constitution. „[7]

Forming this federation of states, the European Union appears, which is suddenly endowed with the entire arsenal of the supranational body.

Supranationalism and cybersecurity

The experts and strategies in the field of information security agree that the critical infrastructures and the command and control systems of the industrial sector / SCADA, represent from an economic perspective, the backbone of any modern or contemporary country. Groups of professional hackers and even some states through their specialized structures have focused on attacks on critical infrastructures to sabotage, decommission or, in some cases, to neutralize them. One such case was identified in 2018, when Israeli intelligence services using a similar but more complex Stuxnet malicious program extracted data on Iran's critical and nuclear infrastructure, precisely using President Hassan Rouhani's cell phone, occasion where the location of the nuclear archives, as well as the deposits of nuclear materials, were exhibited before the General Assembly of the United Nations on September 27, 2018[8].

History of cyber attacks

To be able to state the need to govern a particular space or domain, I consider it necessary to know it, and how it can be better known if not by drawing up an itinerary, history or even a route of events that brought this need to govern space or domain, where the actions have taken place and are still propagating.

As a result, the first media outlet, suspected of being a cyber-attack, on critical industrial infrastructure was in 1982 when the Trans-Siberian gas pipeline exploded where it is alleged that the explosion was triggered by a Trojan that activated by installing it at the control system.

[6] Prof. univ.dr Adrian Liviu-Ivan, Conferința „*O Europă mai sigură*", Universitatea din Oradea, Oradea, 15.01.2019.

[7] Ivan Adrian-Liviu, Transylvanian Review of Administrative Sciences, Vol.4, Nr.22, „*Governance and "European Constitution*", 2008, p.79, http://rtsa.ro/tras/index.php/tras/article/view/382/372, accesat astăzi 30.04.2019.

[8] Consiliul European, Consiliul Europei, *Adunarea Generală a ONU, New York, 27/09/2018*, https://www.consilium.europa.eu/ro/meetings/international-summit/2018/09/27/, accest astăzi 14.02.2019;

Stuxnet, another computer worm with extraordinary capabilities, discovered in 2010, has managed to infect the most secure Iranian nuclear installations using a physical device - an external flash drive such as a USB flash drive. With this installed computer worm, we managed to change the speed parameters of the rotors of nuclear reactors. Following a detailed analysis, it becomes apparent that with a knowledge of the equipment and technologies used, even today, appropriate solutions can be created and tailored to the exact needs of the attacker.

Cyber-attacks against critical infrastructures receive credit and their value or the resources of their services is destabilized. The so-called "cyberwar" has now become a somewhat intrinsic part of international conflicts. All the more so because of its undetectable nature and the potential to cause physical damage without detaching human or mechanized military forces, it is by far a favorite method of attack, increasingly common.

Without analyzing the "black figure" of attacks on critical infrastructures of any state, I can say that there is a growing need for cybersecurity specialists to identify and manage not only security breaches and persistent or hidden attacks.

Even today, although the problem has been publicized, the employees of the military sector use equipment and applications, which have the capacity not only of geo-localization but also of being used remotely or intercepted to follow the activity of the detainees and those with whom interact. It is not a singular case and it is not just about the Romanian, American military personnel, etc. One of the most sensitive cases is given by the conspiracy of secret military bases, the routes followed by their personnel and their identity[9], and another case is similar but with data not so sensitive would be that of the military base from Deveselu where it is US missile shield installed.[10]

As for leaking information from smartphones, this gap is especially given by the use of applications that provide this opportunity, as a result, the data collected from smart communications equipment are in a proportion of 63% mobile phone numbers and a 37% number of device locations. With these meta-data are collected email addresses, bank details, users and passwords. By 2020, the total number of passwords used by automated systems and users will reach ~ 300 billion.

Forecasts show that cyber-attacks on the medical industry will multiply by 400% and organizations will generally fall victim to "ransomware" cyber-attacks at the rate of one organization every 14 seconds and the costs of these types of attacks, estimated in 2019, are of ~ $ 11.5 billion.

In the security context of the European Union, a new element of novelty appears in 2013. The **EU's cyber policy**, to ensure a level of resilience equidistant, real and equal at the level of the Member States, brings to the fore the need to harmonize the legislation oriented on cybersecurity and resilience. Following these tumultuous common interests, the European Commission issues a **Joint Communication** to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *"Cybersecurity strategy of the European Union: an open, secure and secure cyberspace"*[11].

As a result, the European Union is committed to ensuring and reinforcing the efforts of the member countries in this matter and to provide their citizens with access to the Internet resources on a large scale,

[9] Harta Interactivă STRAVA, Baza Militară de la Deveselu, Jud. Olt, 03.05.2019, https://www.strava.com/heatmap#14.04/24.38239/44.07120/hot/all, accesat astăzi 03.05.2019.

[10] Harta Interactivă STRAVA, Baza Militară de la Deveselu, Jud. Olt, 03.05.2019, https://www.strava.com/heatmap#14.04/24.38239/44.07120/hot/all, accesat astăzi 03.05.2019.

[11] Comisia Europeană, *„Strategia de securitate cibernetică a Uniunii Europene: un spațiu cibernetic deschis, sigur și securizat”*, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=JOIN:2013:0001:FIN:RO:PDF, accesat astăzi 22.04.2019.

provided that they ensure the integrity and security of the virtual space and from that perspective the more offensive and resilient attitude to malicious or criminal acts in the cyber sector.

Supranational elitist governance over the cybersecurity sector

The cyber elite is further represented both by the undeniable and desirable capacities of the people active in the professional environments in their diversity as well as its proper function with an advisory role or decision in a problem of information security. The necessity of this concept, elitism, in the area of governance of the information sector, is not only a real need as the states must fulfil their needs and fulfil the primary objective, to protect the territorial sovereignty, from a jurisdictional, geographical point of view and virtual. The decision-makers, in all their nuances, such as the political, financial and why not, the self-declared, recognized or anonymous decision-makers but which have a certain impact in the area of forming public opinion, can take the highest decision-making in terms of societal elitism concerning the impact they have on society and national decision-makers (*no leaders of non-governmental organizations, civil associations, professional associations or religious communities*).

Organizational chart of cybersecurity sectors in cyber space

The regulation of cyberspace in the international space and implicitly in the national space, and the application of the law can not be neglected as soon as the cyberspace is a common (virtual) area of security, freedom and economic prosperity. The possibility of a solution to be implemented for the peaceful solution of the cybersecurity dilemma and avoiding the collision between the need for over-security, *"and to obtain more rights and freedoms in the cyberspace would be that security, freedom and economic prosperity in the virtual environment be universally recognized as fundamental rights of users equally. In principle, optimal governance in cyberspace will be achieved when there is an easily identifiable analogy between the level of security, freedom and prosperity in cyberspace.*"[12].

The domain of cyberspace security governance is supported by nine main pillars, namely: Security Architecture, Security Operations, Cyber Governance, Risk Management, Security Education, Continuing Vocational Training, Security Intelligence, Rules and Standards, Physical Security.

In the current geopolitical and security context in which Romania holds the status of EU member state, I can strongly and confidently say that the progress of the EU in the light of supranationalism is bearing fruit, and the member countries are naturally aligned. It seems that the EU supranational bodies are receiving increased attention from the Member States, and in the last year there has been an increasing discussion of the emergence of an EU army, which should consist of the military resources of the states throughout the Union. In this context, I see fit to readjust the elite theory and the security decision in the act of governing the cyberspace, oriented to technological progress, research and innovation and development of security systems.

[12] Iulian Popa, Teză de doctorat, „*Securitatea și guvernanța spațiului cibernetic contemporan*”, Universitatea Babeș-Bolyai, Școala doctorală „*Relații internaționale și studii de securitate*”, Cluj-Napoca, 2015, pp.133-134.

CHAPTER IV
DIPLOMACY IN THE CYBERNETIC SPACE

Certainly, a mere affiliation with a certain political actor on social platforms such as Facebook or a "tweet" with bits of information can lead not only to the instability of a stock price but to the economic or security instability of a country.

In Romania so far, we have not identified an analysis of this topic, which is why the novelty elements are given by studying both digital and cyber diplomacy concerning the new context of national, European and non-global security. The development of the subject has led to the understanding of the new diplomatic tool with elements related to the cyber area and its use concerning the respect and further application of the traditional diplomatic protocol.

The emergence of public and digital diplomacy was determined by the entry of new actors, both governmental and non-governmental in the international environment, by the development of a new international security agenda and facilitated by the new information and communication technologies. All these are important tools that make their contribution felt in support of broader diplomatic strategies.

Digital diplomacy must get rid of the "*obscure*" label currently in the cyber area and cultivate its own culture with a well-established and balanced role in the science or art of diplomacy. Digital diplomacy needs to focus on areas where it can support broader diplomatic strategies - public diplomacy, networking, information gathering and knowledge management, conflict resolution and mediation - and the evolution of online technologies and platforms and tools that can deliver the most effective results. Existing social media will continue to play a role when used innovatively and creatively, but diplomatic actors should not depend on them. This should include online platforms that promote more intensive use of scenario building techniques, simulation and adaptation of online activities (games, interactive textbooks, etc.). These new tools in the digital diplomacy arsenal will weigh heavily in favor of non-governmental organizations and other civil society groups and communities.

At European level, Romania is highlighted by a pro-active diplomatic participation in the regulation, cyberspace such as the case of the Committee on Employment and Social Affairs and the framework of the Commission for Civil Liberties, Justice and Home Affairs of the European Parliament, where Romanian diplomats and members of the European Parliament were designated as rapporteurs of the different political groups, for the file on the Digital Single Market. The "*Digital Single Market*" act is a very technical document, and given the Commission's competence, the members were recruited within it, who made their contribution focused on the subject of combating illegal content, in any form on the Internet but also on the protection of personal data. Opportunity with which the opinion was requested through "pro-bono" consultancy forms by some specialists in the field. I took part in this working group, where I contributed relevant and particularly useful information regarding the European Digital Single Market report.

Deeply grounded in threats to the security of the union and alliance (*which is becoming increasingly fragile*), increasingly common, complex, destructive and coercive, dealt with through a persuasive diplomatic policy based on military power and often economic alliance, the states are in a position in which they have to assume a new set of rules, policies and procedures. This new form of diplomacy by far different from traditional diplomacy based on human relations is one based on managing the power and security of information in the cyber sector to the same extent as the ability of the entire union, alliance and nation to maintain and protect their core values.

CHAPTER V

INFLUENCES OF A EUROPEAN UNITARY POLICY ON THE SECURITY OF ELECTRONIC INFORMATION IN THE CURRENT GLOBAL GEOPOLITICAL STATE

Studying the implications of digital diplomacy and cyber diplomacy naturally leads us to the need to deepen the influence of European policy on electronic information security in the current global geopolitical state. The first aspect that stands out is the contribution made by the Romanian Presidency and the governmental staff (*MAI, MAE, MECT, etc.*) within the EU as well as the partner states with which our country collaborates.

Romania brings to the foreground, through the official presentation of the Ministry of Foreign Affairs, a statement stating that the official has taken attitude regarding the new trends by adopting the Cybersecurity Strategy of Romania and the MFA actions regarding cybersecurity at a national level, and internationally by the existence of the European Union Directives such as Directive 2016/1148 on measures for a high common level of network and IT security in the Union (entered into force in August 2016).

Cyber resilience can be described as the ability to continuously deliver the desired result, despite adverse cyber events. This ability can be considered at different levels, where each level brings unique challenges, methods and types of conceptual controls concerning cyber resilience. Therefore, the ability to continuously deliver the desired result refers not only to a nation, but also to an organization or even a specific IT system. However, for cyber resilience to be effective, it must be addressed holistically, on multiple levels and in parallel.

Cybersecurity transcends the conventional understanding of the specialized literature in the field of national security concerning international relations. The security dilemma, in this case, is directly caused by the cross-border character of cybercrimes and the need for the cooperation of states through its specialized bodies in the international spectrum. The specialized expertise in the cybersecurity sector and non-state actors in the private sector is required for the help of these bodies. By focusing our attention on the typology of cyber-attacks, we can see that the first response to such attacks comes from the target or victim. Therefore, the general security sector has been privatized all over the world, only the national security being deprived of the eyes of non-state actors.

In order to express this relationship and the capacity for interdependence as coherently as possible, it is necessary to observe at each level of cyberspace governance the challenges, methods and types of unique conceptual controls concerning cyber resilience, understanding the ability to permanently deliver the desired security outcome that refers to an alliance, a nation, an organization or even a specific information system. As it has been found, for cyber resilience to be effective, it must be approached holistically on all existing levels and in parallel.

The elements of novelty are brought by the analysis of the problem of cybersecurity from the perspective of the supranational bodies through the international entities of profile and the involvement of Romania as a proactive member in the field, context in which we conducted a comparative study of cyber resilience and cybersecurity to understand Romania's position in relation to the European Union - EU, North Atlantic Treaty Organization - NATO, COUNCIL OF EUROPE - CoE Organization for Security and Cooperation in Europe - OSCE.

CHAPTER VI

CASE STUDY - CULTURE OF CYBERSECURITY IN ROMANIA

In an overwhelming proportion, almost everything we do, every day, is connected by the cyber domain through modern communications equipment. This phenomenon is the result of technological progress in the sector of communication and information technology.

This extraordinary result of modernization, of technological progress, "*digitalization*" is a central and necessary element of the process of understanding this new age, of globalization. In the same vein, we can say that the democratization of technology is the promoter of globalization of production. I say this because one of the things pursued in this case study is the level and implications brought by the use of modern technologies (*hardware and software*) on the personal, social and professional life of the population of Romania in 2016-2018.

In order to be able to make a statement in the academic environment, in the context of scientific research and to a greater extent in the context of national security, it is necessary to have a knowledge base from which to start a discussion and based on which to argue your exposure. As a result, this last chapter of the thesis is dedicated exclusively to the study of the factor called "*cybersecurity culture*" concerning the topic of the other four thematic chapters (chapters II - chap. IV), to validate and invalidate the hypotheses and to answer to the research questions proposed in the introduction.

The statistical analysis of the cybersecurity culture of the resident population in Romania was also obtained from open sources of information. Of course, such analyses can be made by collecting, evaluating, verifying and centralizing the data from the communications and reports issued by the manufacturers and suppliers of cybersecurity solutions, CERT-RO, the National Institute of Statistics and other national or international bodies. Last but not least, niche researches focused on providing statistical assessments and exposing or resolving security issues in general. As a result, referring to the latest Statistical Briefing of the INS of 2018 we can realize that in the present paper we refer to a final sample of 5,446 persons out of a total of ~ 7,600 questionnaires, which represents ~ 0.03% of the 19,644,350 persons who is the estimated number of resident population in Romania for 2017.

The survey

We start from the consideration that a real, faithful and granular evaluation of the level of cybersecurity culture in Romania cannot be generated only by applying interviews among the elites (*experts, specialists, analysts, teachers, consultants, etc.*) that it works in the cybersecurity sector or the decision- makers or the public / private sector profile institutions. Such an approach would probably generate an assessment of the level of professionalism in relation to the people evaluated in relation to the positioning on the market of the organizations to which they belong, but in no way would they mirror the level of security culture.

Motivated by the considerations set out above and the need to answer the research questions proposed, I considered it appropriate to apply the questionnaire method. The questionnaire is the result of three validation stages. All three forms were subject to analysis in a specialized commission. The persons identified in this commission were chosen on the principle of expertise in the field of specialties practiced by them, namely a sociologist, a psychologist, an expert in national security and an expert in statistical studies.

In order to validate it and to give it a form, the questionnaire was applied to a number of ten specialists in the information and communication technology sector. They unanimously suggested that there was a need for concrete and sufficient technical questions regarding the level of knowledge in the IT&C field to be able to evaluate the level of knowledge of the communication and information management technology in the virtual environment.

A second form was given after another set of 10 questionnaires were applied to experts in the legislative sector who commented and highlighted a need to emphasize cybercrime issues, increasingly identified in the virtual economic sector and beyond.

The third stage of updating and validating the questionnaire questions was marked by the statistical evaluation, which was carried out under the close supervision of the Department of Psychometrics and Statistics within the Faculty of Behavioral and Social Sciences of the University of Groningen, with the help of the resources to which I also completed the statistical study of the applied questionnaires and which guided me step by step until the completion of the statistical study.

Statistical analysis

The data centralization of the questionnaires applied extended over a period of about four months. In the first three months, the data from the applied questionnaires were introduced, which were in paper format. For reasons of authenticity and veracity of the data used in this study, original questionnaires are kept for an indefinite time. Predominantly, the quantitative analysis was at the basis of the qualitative analysis, using at that time the specialized literature and the specialized computer applications in this regard. Regarding the interpretation of the data to obtain a conclusive result in the qualitative analysis, the study and the experience accumulated during the three years offered the expected result, by understanding the degree of a security culture that the resident population in Romania has. It is worth mentioning, regarding the research questions of the thesis, in this context is the fact that this analysis represents a new research possibility, an area of major interest and obtaining a vital indicator on the "barometer" of the cybersecurity culture, of course for the national security.

This process involved identifying and excluding duplicate cases from the database, identifying and excluding cases that contain logically impossible or improbable answers (*for example, users who declared that they were 0 years old or spend more than 24 hours a day using technology*), identifying and excluding the answers of participants too young (*less than 14 years old*) or too old (*over 70 years old*) for this study, and identifying and excluding cases with high rates of missing answers (*for example the cases with no answer for more than 80% of the questions*).

To be able to analyze the data consistently, using the same statistical test to analyze the answers to all questions, the numerical variable "*age*" was transformed into a categorical variable. In this regard, users under the age of 20 were listed as "*young*", those between the ages of 20 and 60 were listed as "*adults*", and those over the age of 60 were listed as "*the elderly*".

Because almost all the questions in the questionnaire used generated nominal data of type through answers of type YES / NO or of ordinal and scalable type (f*or example, the assessment of the importance of computer security on a scale from 1 to 5*), the main analytical strategy we have used was the frequency analysis. The purpose was to determine if there are significant differences between the participants regarding the variables of interest in this study, an example would be the one in which we quantify the extent to which the Romanian users consider digital technology to be important. We also set out to determine if there are associations between certain aspects evaluated in this study, such as the extent to which users have been victims of computer crimes in relation to certain issues related to computer security.

The appropriate statistical test for frequency analysis is the so-called chi-square test, Pearson $\chi 2$. This statistical test can be used to determine whether there are statistically significant differences between observed and theoretical (expected) frequencies within one or more response categories.

All statistical analyses were performed in the R programming language for statistical computing; R1 Core Team, 2019 and SPSS2 v.25 (*R programming language for statistical computing; R*[13] *Core Team, 2019 ans SPSS*[14] *v.25.*

A total of 5,446 people participated in this study voluntarily, in scheduled meetings, face to face, completing the questionnaire. The answers of 52 participants were eliminated from the final analysis of the data because they stated that they were under 14 years of age or older than 70 years. Therefore, for the final analysis of the data, the answers of 5,141 participants representing approximately 94% of the original sample were used. Of these, 3,254 (63.3%) participants provided complete answers to closed-ended questions.

The analysis of the incomplete answers shows that the most missing data (12.5% of the total participants) correspond to the question "*Have you ever attended courses in the computer field?*", followed by the question "*Have you ever been a victim of cybercrime?*" with 7.4% missing answers and the question "*Do you consider that Romania is ready for a possible wave of cyber-attacks?*" with 6.7% missing answers.

The distribution of participants according to gender was given by 53.8% female participants, 46.2% male and 1.5% did not declare gender.

The age of the participants has an asymmetrical distribution to the right, being represented by a median of 23 years, and 75% of the participants are under 35 years. A 2.2% of the participants did not declare their age.

Regarding the environment of origin of the participants, 29.3% of them come from the rural area and 70.7% from the urban area. 6.6% of the participants did not declare their environment of origin.

At the same time, according to the social status, the participants are distributed as follows: students (45.0%, respectively 41.9%), employees and freelancers in similar percentages (5.3%, respectively 5.2%), 2.6% unemployed and no retired people. A percentage of 1.8% of the participants did not declare their social status.

Analysis of the Digital Competences of the Romanian Users

The digital competences of the Romanian users were evaluated through a set of 7 questions that concern aspects such as the level of digital skills, the type and purpose of the digital equipment used, the time spent using digital technology, as well as the perceived importance of digital technology. Time spent using digital technology is considered an indicator because it is related to the degree of vulnerability and risks associated with online platforms or the use of computer resources. Of course, this time of use of technology offers a perspective, on the degree of expertise and adaptability to virtual environments, reporting and even dependence on it.

It was also evaluated the extent to which digital competences are associated with socio-demographic variables such as gender, age (young people under 20 years, adults between 20 and 60 years, older people over 60), environment of origin (urban or rural) and occupation of participants (student, employed student, contractor/freelancer, or unemployed / without occupation). The results of these analyses are presented in the following paragraphs.

Since most security breaches are due to either the lack of digital skills or the lack of security culture, it is considered appropriate to know the user's self-perception regarding his or her level of digital skills.

[13] R Core Team (2019*), „R: A language and environment for statistical computing"*, R Foundation for Statistical Computing, Vienna, Austria, URL: https://www.R-project.org/, accesat astăzi 19.03.2019.

[14] IBM Corp. (2017), „*IBM SPSS Statistics for Windows - Statistical Package for Social Sciences"*, Version 25.0, Armonk, NY: IBM Corp, URL: https://www-01.ibm.com/support/docview.wss?uid=swg24043678, accesat astăzi 19.03.2019.

During the meetings, after completing the questionnaire, I often asked clarification questions. These included "*Do you think you are sufficiently prepared for the technology used?*", and the answers were mostly affirmative. These clarification questions were also asked to cross-check other questions from the content of the questionnaire applied, such as "*Have you ever been a victim of a cybercrime?*" or "*Do you have online accounts that you use with someone else?*". This often resulted in the fact that the level of self-perception about the degree of digital competence or the level of security culture is wrong.

Regarding the declared level of participants' digital skills, more than half of them have an average level of competence, and about one third have a high level.

Regarding the formal training in the computer field, 42.5% of the participants attended specialized courses and 57.5% of them did not attend.

Thus, of those who attended training courses in the computer field, a high percentage are students (48.7%). Also, significantly fewer are self-employed (24.2%), unemployed or unemployed (17.1%) who have taken such courses. Therefore, attending courses in the computer field is associated with an advanced level of digital skills: 49.0% of those who have attended such courses have an advanced level of digital skills. In terms of the number of hours spent using digital technology, on average the users in this sample do this for 5 hours a day. A quarter of participants spend less than 3 hours a day using digital technology, while a quarter is online more than 10 hours a day. Regarding the extent to which this time is spent in the online environment, the data show that half of the respondents spend in the online environment between 50% and 100% of the time spent using digital technology. A quarter of respondents spend less than 50% of their time in the online environment, while a quarter of them spend 100% of their time on digital technology in the online environment.

The use of computer applications is practised in a proportion of 90% by Romanian users, the difference being statistically significant and practically important.

The computer applications mentioned are Facebook, Microsoft Office, WhatsApp, Instagram, online search engines, or various email services. The use of these applications is statistically associated with the age of the users and their socio-economic status, but these associations are negligible. This suggests that Romanians use computer applications to the same extent regardless of age, place of origin or socio-economic status.

Regarding the importance of digital technology for Romanian users, 31.3% of them said that digital technology is important for them, 30.3% said that it is quite important, and 26.5% said that it is very important. The remaining 11.8% stated that for them digital technology is little or not important. The perceived importance of digital technology in Romanians is statistically significantly associated with the environment of origin and the socio-economic status of the users. Users who consider digital technology to be very important come from the urban area in a higher percentage (20.5%) than we would have expected in the absence of the association between variables.

The analysis of the correlation between the perceived importance of digital technology and the socio-economic status of Romanian users shows that, among those who consider digital technology to be not at all important, a higher percentage than we would have expected in the absence of the association are unemployed or freelancers (23.2 %). As far as what is considered by digital technology to be of little importance, most users, more than expected, are unemployed or self-employed (26.7%). For a greater number of students than we expected (66.7%) digital technology is very important, and 33.9% of students consider digital technology to be quite important, a higher percentage than we would have expected in the absence of association of the variables. In other words, we notice that the perceived importance of digital technology differs depending on the socio-economic status of the users. Thus, most students are of high or very high importance to digital technology, while more freelancers and unemployed than we would have expected would be considered as little or no importance. A surprising fact is that students consider digital technology to be very important at a significantly lower percentage (37.0%) and consider it to be little or quite important at a higher percentage (33.3%) than expected. It is also interesting that there is no tendency among employees regarding the perceived importance of digital technology, as their responses are homogeneous.

Regarding the type of digital equipment used, the most used equipment is the "smartphone", corresponding to a percentage of 31.5% of the total answers and being used by 83.3% of the participants. It is followed by laptop and computer (PC), with 28.6% and 22.2% of the total answers. Thus, 75.7% respectively 58.7% of the participants use the laptop and desktop PC. The tablet is used the least (15.7% of the total responses), a percentage of 41.7% of users using this equipment. 5.5% of users also use other equipment, such as smartwatches, smart TVs, drones, or digital cameras. Data shows that, in general, digital equipment such as the "smartphone", laptop, desktop PC or tablet are used by female and male persons in similar proportions, but mainly by adults or young people, students or students, and people from urban areas.

Regarding the purpose of using digital technologies, the correspondents stressed that the purpose of using these modern technologies is given by the desire and the need to use the media and contemporary social channels, with 21.5% of the total answers and being chosen by 80% of participants. Monitoring the criminal activities in the online environment in recent years, we have noticed that the vulnerability of the users of modern technology is represented precisely by breaking the user accounts to obtain confidential information and data, personal and unfortunately sometimes even classified.

70.5% of users use digital equipment for relaxation/ entertainment purposes, 67.6% use them for informational purposes, 51.7% for correspondence, 50.8% use them for online purchases or services, 48.1% use them for professional purposes, and 3.8 % of participants use digital equipment for other purposes. Table no. 2 shows the percentage in which digital equipment is used for various purposes, depending on the socio-demographic variables. Thus, most socio-economic and demographic categories use digital equipment mainly for socialization, relaxation/entertainment, or for informational purposes.

Elderly people also use digital technology for correspondence, and students and employees do this for professional and correspondence purposes as well.

A percentage of 46.1% of the users stated that they provided, by constraint, documents (67.7%), passwords/access accounts (27.7%) and/or confidential information (29.4%).

57.8% of users were notified, by phone or email, that they had won a prize/sum of money without having participated in any contest or raffle. Of these, 83.5% opened the message, 14.6% responded to the message, 8.1% followed the instructions in the message, and 13.8% deleted the message.

Some of the actions and characteristics described above are associated with the socio-demographic variables and/or with the perceived importance of the users' IT security.

Surprisingly, of those who consider computer security to be very important, a larger number than we would have expected (44.6%) subscribe to the different causes using the email address or declare that they have received unsolicited messages by phone or email through who have been notified that they have won a prize or a sum of money, without having participated in any form of competition or raffle.

Moreover, of those who receive such messages or emails, a larger number than we would have expected open these messages even though they say that computer security is very important (49.4% of users who attach high importance to open security the messages received which tell us that either they do not fully understand the notion of computer security or they carry out actions without reasoning the effects and the risks they are subjected to. At the same time, most of those who open this type of messages are students.

Of those who support humanitarian or social campaigns with small amounts of money, a fairly large percentage is given by students (45.9%) or employees and which gives high or very high importance to information security.

Regarding the disclosure by the constraint of passwords/access accounts, the students present a higher risk in this chapter, a percentage of 59.4% of those who stated that they were forced to divulge passwords or access accounts being students.

More students (47.3% of students) and young people up to 20 years old (48.6% of young people) than we would have expected have in their contact list people they do not know.

36.6% of the users have in their circle of friends people victims of computer crimes, and 17.8% of the users were themselves victims of such crimes. Of the latter, 66.6% were victims of computer system infection with malicious applications and programs, 35.2% were victims of personal data theft, and 32.5% were victims of identity theft.

In general, a higher risk of becoming victims of cybercrime are users who: in their circle of friends some people have been victims of cybercrimes, share aspects of their personal lives with strangers, entrust personal data to strangers, provide copies of personal documents, offer or request help with the use of a bank card, have online accounts that they use with someone else, receive messages by phone or e-mail that they have won a prize or sum of money without having participated in any contest or raffle.

Asked if they think Romania is ready for a possible wave of cyber attacks, significantly more users answered in the negative (63.9%).

Among the reasons listed are the lack of specialists and professional training in this field, the lack of funds and the necessary infrastructure, the instability of the computer system or poor information about computer security. Of the users, significantly more believe that it is important or very important to introduce the study of computer security in the pre-university environment (65.7% of users) and the university environment (72.9% of users). These responses are statistically significantly associated with a very high perceived importance of information security, both in terms of introducing these studies in the pre-university environment and the university environment.

Among the reasons why users think it is important or very important to introduce the study of computer security are to protect the identity and personal data, to know the risks exposed by the users of information technologies or to avoid frauds and scams.

Following the model of qualitative research, it is important to mention that during each interview, 27 main questions were evaluated in the complexity of which were reached 57 punctual aspects to which the questionnaire was answered.

CONCLUSIONS

Limitations and future directions of research

The governance of the cyber domain in the context of European security is marked by a strategic evolution of the European reconstruction. I conclude that the cyber domain can be governed by sovereign member states in a European Union balanced between the three governance models: "distributed governance, multilateral governance and multi-stakeholder governance". This does not exclude the strategic partnerships of the member countries or of the Union.

Due to the approach of the exploratory research methods of cybersecurity, I am urged to note that good governance, perceived in the context of this paper, is perfectible and still far from being a universal panacea for the security dilemma in cyberspace. Following an inductive analysis of the results of this paper, I identify the reality of the necessity of building a forum for developing a new model of good governance of the cyber area by associating with this form of government, the government institutions and bodies, the private sector and the civil society actors. I am fully confident that the present thesis has opened up new horizons for scientific research of good governance in the cyber space. With the motivation given by identifying these horizons, which are otherwise tangible, as well as the achievement of the proposed objectives in part, I intend that the results obtained in this thesis will be the basis for further extensions of the present research and bring to the attention of the academic community, new perspectives and results regarding good governance of cyberspace security.

By referring to the other four strategic areas identified, the study of good governance in the cyber space represents at present the most deficient area where, in terms of national security, we have identified a particular need for democratic control by the civil society, as a result or an action obtained in the assent of supranational or national institutions. The problem of escalating the security spiral is for me a major point of interest, intending for the future to research real possibilities and hypotheses with the help of which a new form of good governance of the cyber space can solve aspects of the security dilemma.

Finally, in terms of motivating the choice of future research directions, a final argument is given by the strategic approach of the last ten years that I foster on researching the field of national security in cyber context, through the dynamic ability of the three elements to change direction or the rules during the game, namely: technological progress, international relations and security.

Details about personal contributions

Starting from the understanding of a need for impartiality on the part of the researcher, I detached myself from any influences that could affect the natural and objective course of the paper. Without contesting the fact that, at any time, subjectivity, even to a negligible extent, may arise due to our human nature and belonging to a particular group or social class, noting that from the beginning, the analysis and approach of the problem has been carried out to a raised degree of difficulty, finally materializing according to the author's vision, using a mechanism of analysis, synthesis and systematic generation of the results confirming them by verifying them in the light of the comparative study. For a better conceptualization and understanding of the research, the novelty elements are exposed at the end of each chapter, reiterating in the following by a common conclusion, regarding the whole study.

The main element of novelty and originality brought to the field of research in which the present thesis is inscribed is given by obtaining an interdependence relation between the security culture, the level of existing national security and the way of cyberspace governance.

A secondary element of novelty is given by the construction of a structured case for demonstrating the solid arguments supported by the security culture level in Romania in relation to the management of information transmitted in the electronic environment for good governance of cyber space in a national and predominantly European context. The lack of specialized bibliographic sources oriented in the direction of the problem of cybersecurity spirals, offers a validation of my approach, realized under the careful monitoring of the coordinating teachers. The validation and confirmation of this exploratory research approach is given by obtaining concrete results, in favor of the hypothesis that the cybersecurity dilemma is a hybrid sub- dimension or terminology, differentiated from the usual meaning of the security dilemma by its conceptual transposition into the context of cybersecurity.

Essentially, by assuming the results of the research of the cybersecurity dilemma in the perspective of virtual space governance in the concept of realism and supranationalism, I understand that, in the next decade, until the next revolution of technology in the cyber space, the role of public, private, national and supranational bodies, it is the norm to regulate this area in order to diminish the impact brought by the security risks in all the environments on which the security dilemma makes its presence felt. Although a large-scale military offensive through the cyber environment is unlikely, isolated cases with a huge financial impact and intimidation of both legal entities and people using this environment are becoming more and more frequent. Analyzing from the perspective of the studies of international relations, the diplomacy has reached a new threshold, that of transformation and acquires in the portfolio a new areas of interest, cyber diplomacy and digital diplomacy that represent in the context of globalization, the interface of states, which is also one of the sources generating main security.

A final consideration is that regarding the future obligation of non-proliferation of potentially hostile cyber capabilities. Through the examples given and the study of their effects on states and alliances, it is partially confirmed, the possibility identified at the theoretical level of using cyber-attacks globally in order to produce massively harmful effects from the states. However, I am fully confident that through good governance and increasing the cyber resilience of information systems, globally, and at the same time, through active participation of states, unions, federations and alliances for harmonization and regulation consensual to this field, it can be maintained regardless of the ideology of state governance, a safe and clean cyber environment.

The central thread of the author's vision is given by identifying a new perspective on cyberspace security management. The basic elements of this new perspective are highlighted both by the keywords from the beginning of the paper and as definitive, in the content of the chapters of this thesis. Of course, in the author's view, this perspective represents a new analysis framework and an element of novelty that can shed light on the future research directions in the field of international relations sciences and security studies.

Also, in the context of the present paper, due to its multidisciplinary nature, this new perspective of analysis mentioned above, I think it can contribute to the identification of new challenges in the field of research and studies of diplomats and those in the area of communications and information technology.

The approach of the chosen theme was initially studied and researched in order to bring the knowledge of the academic community in a scientific point of view and to try to transpose the problematic through the concepts of realism and supranationalism. The validation of the study is, of course, left to the critics and in hope of constructive reactions the author's wish is to develop, in whole or in part, the chosen research topic.

BIBLIOGRAPHY

Given the considerable volume of bibliographic materials used throughout the study, the following will be listed the most important bibliographic resources relevant to the research topic.

BOOKS (*including electronic editions*)

- Adrian V. Cămărășan, Informații clasificate – Note de curs, Ed. CA Publishing, Cluj-Napoca, 2014.
- Adrian-Liviu Ivan, Colecţia Studii Europene, „Statele Unite ale Europei: Uniunea Europeană între interguvernamentalism şi supranaţionalism”, Editura Institutul European Iaşi, Iaşi, 2007.
- Alexandra Sarcinschi, „Elemente noi în studiul securităţii naţionale şi internaţionale”, Editura Universităţii Naţionale de Apărare, Bucureşti, 2005.
- Andreas Schmidt, The fierce domain –conflicts in cyberspace 1986-2012, „The Estonian Cyberattacks”, Ed. Atlantic Council, Washington, D.C, 2013.
- Annette Freyberg-Inan, What Moves Man: The Realist Theory of International Relations and Its Judgement of Human Nature, Ed. State University of New York Press, Albany, SUA, 2004.
- Anișoara Duică, Management, Ediția a II-a (revizuită și adăugită), Ed. Bibliotheca, Târgoviște, 2008.
- Anthony J.S. Craig, Brandon Valeriano, „Realism and Cyber Conflict: Security in the Digital Age”, Ed. E-INTERNATIONAL RELATIONS PUBLISHING, Bristol, Anglia, 2018.
- Arnold Wolfers, Political Science Quarterly, Vol.67, Nr. 4, „National Security as an Ambiguous Symbol”, Ed. Academy of Political Science, New York, SUA, 1952.
- Barry Buzan, „Popoarele, statele şi teama. O agendă pentru studii de securitate internaţională în epoca de după Războiul Rece”, Ed. Cartier, Chișinău, 2000.
- Barry Buzan, Ole Wæver, Jaap de Wilde, „Securitatea. Un nou cadru de analiză”, Ed. CA Publishing, Cluj-Napoca, 2011.
- Bogdan Băcanu, „Organizați publică – Teorie și management”, Ed. Polirom, Iași, 2008.
- Cavelty Myriam Dunn, „Cyber-Security and Threat Politics: US efforts to secure the information age”, CSS Studies in Security and International Relations, Prima Ediție, Ed. Routledge, London, UK, 2008.
- Ciprian Nițu, „Cosmopolitismul-Către o nouă paradigmă în teoria politică”, Ed. Adenium, Iași, 2014.
- Clarke A.Richard, Robert K. Knake, „Cyber War: The Next Threat to National Security and What to Do About It”, New York: Ecco, SUA, 2010.
- Clifford Paul Stoll, „The Cukoo's Egg: Tracking a Spy Through the Maze of Computer Espionage”, New York, Doubleday, 1989.
- Colin Robson, „Real World Research: A resource for Social Scientists and Practitioner-Researchers”, Cap. II.6. Flexible Design, Ediția a-II-a, Anglia, Ed. Blackwell Publisher, Oxford, 2002.
- David Wright-Neville, „Dicționar de Terorism”, Traducere Sorina Pricop, Ed. CA Publishing, Cluj-Napoca, 2010.
- Dumitru Oprea, „Protecția și securitatea informațiilor”, Ediția a II-a, Ed. Polirom, Iași, 2007.
- George Christou, New Security Challenges, „Cybersecurity in the European Union - Resilience and Adaptability in Governance Policy”, Ed. Palgrave Macmillan, 2016.
- Georgeta Chirlesan , „Strategia de securitate naţională a României: evoluţii şi tendinţe între securitatea regională şi cea euro-atlantică”, Editura Academiei Forțelor Terestre „Nicolae Balcescu”, Sibiu, 2013.
- Gheorghe Ilie, „De la management la guvernare prin risc”, Ed. Detectiv/Ed. UTI Press, București, 2009.
- Gheorghe Ilie, Ion Ciobanu, Aurel Nour, „Confruntarea informațională și protecția informațiilor”, Ed.Detectiv, București, 2006.
- Gheorghe Ilie, „Riscul-Măsura Incertitudinii – Elemente conceptuale, corelații și determinări” -, Ed. UTI Press, București, 2011.

- Ioana Vasiu, Lucian Vasiu, Criminalitatea în cyberspațiu, Ed. Univers Juridic, București, 2011.
- Ioana Vasiu, Lucian Vasiu, Informatică Juridică și Drept Informatic, Editura Albastră, Cluj-Napoca, 2009.
- Ionel Nițu, „Analiza de Intelligence, O abordare din perspectiva teoriilor schimbării”, Ed. Rao, București, 2012.
- Jervis Robert, World Politics, Vol.30, Nr.2, „Cooperation Under the Security Dilemma”, Ed. The Johns Hopkins University Press, 1978.
- Jonathan Grix, „Demistificarea cercetării postuniversitare: De la masterat la doctorat”, Traducere de Nicolae Melinescu, Ed. CA Publishing, Cluj-Napoca, 2014.
- Lillian Ablon, Anika Binnendijk, Quentin E. Hodgson, Bilyana Lilly, Sasha Romanosky, David Senty, Julia A. Thompson, PE-329-NATO, „Operationalizing Cyberspace as a Military Domain: Lessons for NATO”, Ed. RAND Corporation, Santa Monica, USA, 2019.
- Mary Kaldor, „Securitatea Umană”, Ed. CA Publishing, Cluj-Napoca, 2010.
- Mihaela Vlăsceanu, Organizația: proiectare și schimbare – Introducere în comportamentul organizațional, Ed. Comunicare.ro, București, 2005.
- Morgenthau Hans J., ”Politics among Nations: The Struggle for Power and Peace”, New York, Ed. Alfred A. Knopf, 1949.
- Nasty Vlădoiu, „Protecţia Informaţiilor, De la concept la implementare”, Ed. Tritonic, București, 2005.
- Martin Griffiths, „Relaţii internaţionale. Şcoli, curente, gânditori”, Traducere: Cristea Darie, Popistaşu Olga, Barna Cristian, Editura Ziua, Bucureşti, 2003.
- Mireille Rădoi, Serviciile de informații și decizia politică, Ed. Tritonic, București, 2003.
- Norman Blaikie, Colecția Sociologie, „Modele ale cercetării sociale: Producerea cunoașterii”, Ediția a II-a, (Trad. Coca Vieru, Ana Gruia), Ed. CA Publishing, Cluj-Napfoca, 2010.
- Nye Joseph S., „The Future of Power”, New York, Ed. Public Affairs, 2011.
- Nye Joseph S., Foreign Policy, Nr.80, “Soft Power”, Washington, Ed. Washingtonpost, Newsweek Interactive, LLC, 1990.
- Ole Wæver, „Securitization and Desecuritization’, Rev. Ronnie D. Lipschutz „On Security”, Ed. Columbia University Press, New York, 1995.
- Paul Robinson, „Dicționar de securitate internațională”, Traducere Monica Neamț, Ed. CA Publishing, Cluj-Napoca, 2010.
- Penelope Hartland-Thunberg, National Economic Security: Perceptions, Threats, and Policies: “National Economic Security: Interdependence and Vulnerability”, Ed. John F. Kennedy Institute, Olanda, 1982.
- Robert K. Yin, „Case Study Research: Design and Method, Ediția a-V-a”, SUA, California, Thousand Oaks, Ed. SAGE Publications, 2014.
- Rid Thomas, „Cyber War Will Not Take Place” Londra, UK, Ed. C Hurst & Co Publishers Ltd., 2013.
- Russett Bruce, John Oneal, Triangulating Peace, Democracy, Interdependence, and International Organizations, New York-Londra, Ed. W.W. Norton & Company, 2001.
- Senese Paul D., John A. Vasquez, „The Steps to War: An Empirical Study”, Ed. Princeton University Press, Princeton, SUA, 2008.
- Shaun Riordan, „The Strategic Use of Digital and Public Diplomacy in Pursuit of National Objectives”, Ed. Top Open Printing Sytems S.L., Barcelona, 2016.
- Thomas L. Friedman, „The Lexus and the Olive Tree – Understanding Globalization”, Ediția revizuită, Ed. Farrar, Straus and Giroux, New Yok, SUA, 2000.
- Țicu Dorina, „Politicile publice. Raționalitate și decizie în spațiul administrativ”, Ed. Adenium, Iași, 2014.
- Vasquez A. John, „The War Puzzle”, revizuită de Thomas B. Mackie, Cambridge, Cambridge, Ed. Cambridge University Press, 1993.

- Waltz Kenneth N., „Theory of International Politics”, Londra, Ed. Addison-Wesley Publishing Company, 1979.

SCIENTIFIC ARTICLES AND CHAPTERS IN BOOKS (*including electronic editions*)

- Adrian Liviu-Ivan, Hello World!: Contemporaneitate și provocările globalizării, CRIISS/1, „Constructivismul și Integrarea Europeană: Contribuții și Limite”, Ed. CA Publishing, Cluj-Napoca, 2014, p.146.
- Alexander Klimburg, Hugo Zylberberg, NUPI Report nr.6, “Cybersecurity Capacity Building: Developing Access”, Ed. Norwegian Institute of International Affairs, Oslo, Norvegia, 2015, p.23.
- Alexandru Nicolae CLAIN, Revista „Continuitate și schimbare în guvernanța europeană”, Vol. 4, Nr. 1, „Consiliul Europei – instituţie supranaţională sau conferinţă interguvernamentală?”, p.14, http://europolity.eu/wp-content/uploads/2014/05/Vol.4.1.-2010.pdf, accesată astăzi 04.05.2019.
- Andreea-Maria Tirziu, MPRA Munich Personal RePEc Archive, „Protection and security of information at the level of national public authorities from Romania”, p.127, https://mpra.ub.uni-muenchen.de/77711/1/MPRA_paper_77711.pdf, accesat astăzi 14.03.2019;
- Andrew N. Liaropoulos, Democracy and an Open-Economy World Order, „Cyberspace Governance and State Sovereignty”, Ed. Springer International Publishing AG, p.29, https://www.researchgate.net/publication/316040640_Cyberspace_Governance_and_State_Sovereignty, accesat astăzi, 07.05.2019.
- Anthony Craig, Brandon Valeriano, „Conceptualising cyber arms races”, 8th International Conference on Cyber Conflict (CyCon), Ed. NATO CCD COE Publication, Tallin, 2016.
- Anton Rog, Cristian Condruț, Intelligence în serviciul tău, Nr.38, „Evoluția amenințării cibernetice”, Ed. SRI, București, 2019, pp.10-11.
- Aurelia PERU-BALAN, Vitalina BAHNEANU, MOLDOSCOPIE, Nr.1, Vol. LXXX, Războiul informațional, Propaganda, Fake-News: Controlul asupra percepției publice, Chișinău, 2018, pp.129-131.
- Arquilla John, Ronfeldt David, „Comparative Strategy”, Vol.12, Nr.2, “Cyberwar is Coming!”, 1993, pp.141–165.
- Aseema Sinha, International Studies Review, Vol. 20, Nr. 2, „Building a Theory of Change in International Relations: Pathways of Disruptive and Incremental Change in World Politics”, Ed. Oxford University Press, Oxford, Regatul Unit, 2018, pp.195–203.
- Avidit Acharya, Kristopher W. Ramsay, Quarterly Journal of Political Science, “The Calculus of the Security Dilemma”, Vol. 8, nr. 2, Princeton, USA, 2013, pp. 184-185.
- Babak Bashari Rad, Nafisseh Akbarzadeh, Pouya Ataei, Yasaman Khakbiz, International Journal of Control Theory and Applications, Vol. 9, nr.43, „Security and Privacy Challenges in Big Data Era”, 2016, pp.438-441, https://www.researchgate.net/publication/327111196, accesat astăzi 11.08.2019.
- Björck F., Henkel M., Stirna J., Zdravkovic J. (2015) „Cyber Resilience – Fundamentals for a Definition”. In: Rocha A., Correia A., Costanzo S., Reis L. (eds) New Contributions in Information Systems and Technologies. Advances in Intelligent Systems and Computing, vol 353, Ed. Springer, Cham, pp.311-312;
- Brandon Valeriano, International Interactions Vol. 35, Nr.2, „The Tragedy of Offensive Realism: Testing Aggressive Power Politics Models”, Londra, Anglia, 2009, Ed. Routledge Taylor&Francis Group, p.180.
- Cătălina Todor, Strategic Impact, Vol.63, Nr.2, „The topicality of security dilemma’s spiral model in analysing the international environment”, București, 2017, Ed. “Carol I” National Defence University Publishing House, p.25.
- Charles L. Glasser, The Perils of Anarchy: Contemporary Realism and International Security, „Realists as Optimists: Cooperation as Self-Help”, Ed. The MIT Press, Massachusetts, 1995, pp.336-340.

- Charles L. Glaser, Chaim Kaufmann, International Security, Vol. 22, nr. 4, „What is the offense-defense balance and can we measure it? (Offense, Defense, and International Politics)", 1998, Massachusetts, Ed. Massachusetts Institute of Technology, p.44.
- Corneliu Bjola, Global Affairs, Vol.2, Nr.3, Digital diplomacy – the state of the art, Ed. Routledge Taylor & Francis Group, 2016, https://doi.org/10.1080/23340460.2016.1239372, pp.297-298.
- Cristian Niţă, Securitatea Naţională – O Perspectivă Academică, p.3, http://www.nos.iem.ro/bitstream/handle/123456789/33/4.1.Sec%20Academic%20nita.pdf?sequence=1&isAllowed=y, accesat astăzi 30.07.2019.
- Cristopher Daase, Theories of International Relations, „The English School", Ed. Routledge Taylor & Francis Group, Londra, 2014, pp.150-151.
- Damien van Puyvelde, Stephen Coulthart, Shahriar M. Hossain, International Affairs Vol. 93, Nr.6 „Beyond the buzzword: big data and national security decision-making", https://doi.org/10.1093/ia/iix184, 2017, p.1400.
- Deborah J. Bodeau, Richard Graubart, MITRE Tehnical Report (2011), "Cyber Resiliency Engineering Framework", Bedford, Massachusetts, SUA, 2011, p.37.
- Dumitru Iancu, Anuarul Academiei Fortelor Terestre "Nicolae Balcescu", Informaţia–Sursã de avantaj concurenţial, 2007, http://www.armyacademy.ro/biblioteca/anuare/2007/a21.pdf, accesat astăzi 23.07.2019.
- Emily Goldman, John O.Arquilla, Defense Analysis, „Cyber Analogies", Ed. Naval Postgraduate School, Monterey, California, 2014, http://hdl.handle.net/10945/40037, accesat astăzi 05.05.2019.
- Erica Moret, Patryk Pawlak, Brief SSUE, 24/2017, „The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime?", https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%2024%20Cyber%20sanctions.pdf, accesat astăzi 04.03.2019;
- Eriksson Johan, Giampiero Giacomello, International Political Science Review Vol. 27, nr. 3,"The Information Revolution, Security, and International Relations: (IR) Relevant Theory?", 2006, pp. 228–229.
- Fredrik Björck, Martin Henkel, Janis Stirna, Jelena Zdravkovic, New Contributions in Information Systems and Technologies, Advances in Intelligent Systems and Computing, Vol.353, „Cyber Resilience – Fundamentals for a Definition", Ed. Springer, Cham, 2015, p.313.
- George-Marius Șinca, AGORA International Journal of Juridical Sciences, Nr.1, „Cibercriminologia - O analiză succintă a fenomenului de tranziție de la criminalitatea tradițională la cibercriminalitate", Oradea, 2015, p.66.
- George-Marius Șinca, De la Elitele Securității la Securitatea Elitelor, „Managementul Elitelor în Managementul Riscurilor Cibernetice", Ed. Presa Universitară Clujeană, Cluj-Napoca, 2017, pp.65-82.
- Georgeta Ghenghea, Zinaida Stratan, Natalia Zavtur, Impactul culturii informaţiei asupra utilizatorilor doctoranzi (studiu de caz), pp.42-45, 2019, http://repository.utm.md/handle/5014/1667, accesat astăzi 23.07.2019.
- Gortzak Yoav, Haftel Z. Yoram, Kevin Sweeney, Journal of Conflict Resolution Vol. 49, Nr.1, "Offense-Defense Theory: An Empirical Assessment", Ed. Sage Publications, Inc., Ohio, SUA, 2005, pp.67–89.
- Harald Cramér, Capitolul 2. Linear Point Sets, „Mathematical Methods of Statistics", Ed. Princeton University Press, 1946, SUA, Princeton, pp.10-14;
- Ilan Manor, Elad Segev, Ronit Kampf, The Hague Journal of Diplomacy Vol.10, nr.4, „Digital Diplomacy 2.0? A Cross-national Comparison of Public Engagement in Facebook and Twitter", DOI: 10.1163/1871191X-12341318, Haga, 2015, p.331.
- Iulian Popa, Teză de doctorat: „Securitatea și guvernanța spațiului cibernetic contemporan", Universitatea Babeș-Bolyai, Școala doctorală „Relații internaționale și studii de securitate", Cluj-Napoca, 2015, pp.133-134.

- Iulian F. Popa, Globalizare. Identitate. Securitate, Metoda scenariilor în analiza informațiilor de securitate națională. Studiu teoretic-aplicativ, Cluj-Napoca, CA Publishing, 2015, pp. 157-178.
- Ivan Adrian-Liviu, Transylvanian Review of Administrative Sciences, Vol.4, Nr.22, „Governance and "European Constitution", 2008, p.79, http://rtsa.ro/tras/index.php/tras/article/view/382/372, accesat astăzi 30.04.2019.
- Jeffrey W. Taliaferro, International Security, Vol.25, Nr.3, Security Seeking under Anarchy: Defensive Realism Revisited, Ed. The MIT Press Journals, Massachusetts, 2000, p.128-161, https://www.mitpressjournals.org/doi/10.1162/016228800560543, accesat astăzi 05.05.2019.
- Joyce, A. L., Petit, F. D., Phillips, J. A., Nowak, L. B., Evans, N. J., Raport Tehnic OSTI.gov, „Cyber Protection and Resilience Index: An Indicator of an Organization's Cyber Protection and Resilience Program", Global Security Sciences Division, Argonne National Laboratory, SUA, 2017, https://publications.anl.gov/anlpubs/2018/03/140164.pdf, accesat astăzi 05.05.2019.
- Kristin M. Lord, Travis Sharp, Vol.1, America's Cyber Future, Security and Prosperity in the Information Age, Ed. Center for a New American Security, Washington, DC, SUA, 2011, https://s3.amazonaws.com/files.cnas.org/documents/CNAS_Cyber_Volume-I_0.pdf, accesat astăzi 05.05.2019.
- Léon Bottou, Frank E. Curtis, Jorge Nocedal, Vol. 60, Nr. 2, „Optimization Methods for Large-Scale Machine Learning", https://doi.org/10.1137/16M1080173, SIAM Review, 2018, pp. 223-311;
- Lieber Keir, Cyber Analogies, "The Offense-Defense Balance and Cyber Warfare", Monterey, California, SUA, 2014, Ed. Calhoun: Institutional Archive of the Naval Postgraduate School, p.96.
- Lori Murray, John Budenske, Shubhagat Gangopadhyay, Robert K.Finstad, Proceedings of the SPIE Defense + Security, Vol.10651, „Cyber resilience and integrity self-awareness of mobile autonomous systems", Orlando, Florida, SUA, 2018, p.8, https://www.spiedigitallibrary.org/conference-proceedings-of-spie/10651/2307854/Cyber-resilience-and-integrity-self-awareness-of-mobile-autonomous-systems/10.1117/12.2307854.short?SSO=1, accesat astăzi, 01.05.2019.
- Mearsheimer John Joseph, International Relations Theories: Discipline and Diversity, "Structural Realism". revizuit de Tim Dunne, Milja Kurki, Steve Smith, Oxford, Anglia, Ed. Oxford University Press, 2006, pp.71–88.
- Radu-Sebastian Ungureanu, Radu-Alexandru Cucută, New Challenges to the Balkan Security - Thematic Collective Book, Vol.3, „EUROPENIZATION AS A HEGEMONIC PROJECT: EU INFLUENCE IN APPROACHING THE SECURITY ISSUES IN THE BALKANS", Ed. Ivis, Veliko Târnovo, Bulgaria, 2016, p.169.
- Teodor Frunzeti, Cristian Bărbulescu, Academia Oamenilor de Știință din România, Cultura de securitate și reziliența națională la amenințările hibride , Reziliența național la amenințările hibride și cultura de securitate. Un cadru de analiză., p.4, http://www.aosr.ro/wp-content/uploads/2019/03/Anexa-1_Articol-Impact-Strategic-2018.pdf, accesat astăzi 23.07.2019.
- Theodor Mitu, Daniela Mitu, Revista Română de Studii de Intelligence, nr. 4, „OSINT – la grania dintre secret și public", București, Ed. Serviciul Român de Informații, 2010, pp.42-43.
- Valeriano Brandon, Ryan C. Maness., „Cyber War versus Cyber Realities: Cyber Conflict in the International System", New York, SUA, Ed. Oxford University Press, 2015, pp.164-187.
- Vasquez John, „The American Political Science Review", Vol.91, Nr.4, "The Realist Paradigm and Degenerative versus Progressive Research Programs: An Appraisal of Neotraditional Research on Waltz's Balancing Proposition", 1997, pp.899–912.
- Vesa Kanniainen, HECER Discussion Paper No. 424, „Cyber Technology and the Arms Race", Helsinki, 2018, pp.1-2.
- William Arthur Conklin, Dan Shoemaker, The EDP Audit, Control, and Security Newsletter, Vol.55, Nr.2 "Cyber-Resilience: Seven Steps for Institutional Survival", Ed. Taylor & Francis Group, 2017, pp. 14-22.

- Wojciech Samek, Klaus-Robert Műller, Explainable AI: Interpreting, Explaining and Visualizing Deep Learning, LNAI11700, DOI.ORG/10.1007/978-3-030-28954-6, „Towards Explainable Artificial Intelligence", Ed. Springer, Elveția, Cham, 2019, pp.8-9.
- Cristian Barna, Intelligence, Nr.35, „Pregătire şi formare în societatea cunoaşterii.", Bucureşti, 2017, Serviciul Român de Informaţii, pp.26-27.
- EEAS, Strategie globală pentru politica externă şi de securitate a Uniunii Europene, http://europa.eu/globalstrategy/sites/globalstrategy/files/eugs_ro_version.pdf, accesat astăzi 04.07.2018