BABEȘ-BOLYAI UNIVERSITY
Faculty of History and Philosophy

International Relations and Security Studies Doctoral School

Doctoral thesis

***

THE SECURITY AND GOVERNANCE OF CONTEMPORARY CYBERSPACE

Doctoral supervisor,

Professor Michael SHAFIR, Ph.D.

Author,

Iulian Florentin POPA

Cluj-Napoca

2015

TABLE OF CONTENTS

SUMMARY

Although in the past few years we have witnessed a relatively peaceful evolution of cyberspace, there are sufficient reasons for which cyberspace governance might be among the most serious issues currently confronting the international community. Beyond any doubt, the cyberspace tends to become an environment of global insecurity. I underscore that the relationship between cybersecurity and cyberspace governance is of vital importance for adopting efficient strategies and policies regarding the cyberspace. My thesis borderlines the neoliberal institutionalism promoted by Robert Keohane[1] and Hobson's neoliberalism[2], as I strongly believe *complex interdependence sometimes comes closer to reality than does realism*[3]. Hence I underscore that the good governance of cyberspace is rather a set of mechanisms and actions aimed to optimize the balance of cyber power for the cyberspace's sustainable and peaceful development, by controlling the interaction of international actors via the principles of good governance I have identified and analyzed below.

Generally I have tested whether the maintenance of the optimum cyberspace security is fundamentally linked to the (good) governance of cyberspace. Even if scientific research concerning cyberspace has registered substantial processes so far, I have surprisingly remarked that many of the academics have omitted to properly study the interdependencies existing between the quality of cyberspace governance and the general cybersecurity level felt by everyone.

Therefore, my objective was to research the relationship between cybersecurity and cyberspace governance, in order to confirm or deny the existence of an interdependence between the level of cybersecurity and the quality of cyberspace governance. Additionally, I have coined a series of conceptual clarifications concerning the cyber lexicon and I have studied whether the cybersecurity dilemma can be solved peacefully via good governance.

I started my research bearing in mind the general hypothesis according to which good governance can contribute to the prevention and the peaceful resolution of the cybersecurity dilemma.

[1] Robert Keohane, *After Hegemony: Cooperation and Discord in the World Political Economy*, Princeton, Princeton University Press, 2005, *passim.*
[2] John Atkinson Hobson, *The State and International Relations*, Cambridge, Cambridge University Press, 2000, p. 65.
[3] Robert Keohane, Joseph Nye, *Power and Interdependence: World Politics in Transition*, Boston, Little, Brown and Company, 1989, p. 23.

Therefore, depending on the consistency of this hypothesis, I have generally assessed whether there is any sort of interdependence between the security and the quality of cyberspace governance. The secondary objective was to identify the main reasons for which we might consider the cyberspace a strategic domain alongside land, air, sea and space.

Given the research strategy I have adopted, I have chosen to state the research hypotheses distinctly, within each chapter. I would like to mention that the secondary research hypotheses had a crucial role in formulating answers to the following research questions:

Q1. To what extent the cybersecurity dilemma might be solved peacefully?

Q2. How can good governance efficiently contribute to the peaceful resolution of the cybersecurity dilemma?

First and foremost I consider that the security and governance of cyberspace should be of vital interest for the academia. I suggest that the dynamics of recent international events such as "The Arab Spring" or "The Twitter Revolution" show that the proper understanding of the phenomena which take place on the "cyber arena" is particularly important for the study of contemporary international relations and security.

Concerning the selection of the topic, I have taken into consideration that many of the current users and even stakeholders have a distorted view (so to speak) on the importance of security and governance of cyberspace. Therefore I couldn't neglect that such research topic is a good opportunity for me to direct the attention of those interested towards the essential role of the security and governance for the sustainable development of cyberspace.

From an academic point of view, my thesis continues and extends the introductive and apparently eclectic research I have undertaken as part of my M.A. studies at Babeş-Bolyai University, studies which were finalized with a dissertation paper on cyberbullying[4]. As it can be seen, it is not an accident that I have chosen to research the security and governance of contemporary cyberspace. Furthermore, I have chosen this field of research because of my desire to use on a scientific level my professional background in the field of IT consulting, intelligence analysis and trends assessment. Also, I couldn't overlook the fact that the current number of cyber researchers in the field of international

[4] Iulian Popa, Dacian Duna (coord. ştiinţific), *Violența cibernetică: Între război convențional și terorism (lucrare de disertație),* Cluj-Napoca, Universitatea Babeş-Bolyai, 2012.

relations and security studies does not match Romania's needs – a country with considerable euro-Atlantic ambitions, at least in the field of cybersecurity.

As concerning the research methodology, it does not fit a certain model, specific only to the study of international relations. I strongly believe that some interdisciplinary methods of research and analysis – not necessarily typical – can contribute in a significant fashion to the development of many analytical products which are sensibly more substantial[5]. Therefore, although I have closely followed all the methodological rigors imposed by such scientific work, I could not neglect the risk posed by the methodological "automatisms" which might spoil the research and analysis[6]. In fact, the methodological stereotypes may stop the researcher or the analyst from making use of the invaluable "weak-signals". Hence I have chosen an analysis methodology that has allowed me to use both the empirical and scientific perspectives of generating knowledge and showed in a better fashion my personal contribution.

Because of the research strategy I have chosen, the thesis was not limited to the analysis of proofs that confirm dominant hypotheses, but rather was focused on mapping and assessing the hypotheses and sources which come into contradiction with the status quo. Both the research hypotheses and the qualitative or quantitative arguments in favor (or against) have been collected from current practices and literature, through direct or indirect data collection and qualitative/quantitative research. The relevance and credibility of the sources have been continuously assessed by consulting experts having vast experience in the field of cybersecurity and cyberspace governance.

The main method used for the analysis was the "analysis of concurrent hypotheses" (ACH) method, which was used in a simplified and customized fashion. To prevent and eliminate possible errors I have used on an experimental basis the ACH 2.05 software program developed by Palo Alto Research Center. In particular, I have utilized the case study method (by putting together several SWOT analyses) in order to test and verify the preliminary research results.

For reasons of academic neutrality I have closely complied with the the principle of causality and complementarity of the research, the principle of correspondence of the research, and the principle of empirical observations via permanent consultations with

[5] Ionel Nițu, „Metode și proceduri utilizabile în analiza de intelligence", în *Ars Analytica – Provocări și tendințe în analiza de intelligence,* George Cristian Maior și Ionel Nițu (coord.), București, Editura RAO, 2013, pp. 205-218.
[6] *Ibidem.*

security practitioners and extensive study of the reports belonging to several governmental agencies and bodies or strategic analysis centers, Ph.D. thesis, scientific papers, magazines, thematic online publications, handbooks, declassified information, and other documents declassified due to leaks of information to public.

1st Chapter

The first chapter is strictly a theoretical one, as I have analyzed the general literature dealing with cybersecurity and cyberspace governance. Without resorting to a certain chronology, I have chosen a dialectical presentation of the academic knowledge because, very likely, *the classical lines of conceptual delimitation* between the contemporary strategic studies paradigms *tend to be more flexible*[7].

In addition, beyond my personal contribution to the cyber lexicon, I have identified the most important arguments according to which cybersecurity is of vital importance for the sustainable development of any society and/or organization. Not the least, I have assessed the conditions under which cyber-attacks may be assimilated to the use of armed force to produce serious material damage and human casualties (directly or not) by disrupting critical infrastructure and terminals.

2nd Chapter

Starting from the observation that cyberspace is a hotbed of insecurity but also an important generator of opportunities, I analyzed whether the cybersecurity dilemma exists and differs from the classic security dilemma.

Therefore, the second chapter focuses on the study of what I have generically labeled "the strategic cybersecurity dilemma" or "the cyber defense dilemma", respectively „the tactical cybersecurity dilemma" or „the temptation of over-security while at peace". For the reasons above, I have identified the reasons for which cybersecurity shows up and differs from the classic security dilemma. In particular, I have identified consistent clues according to which is it not the initiation and rise of the cybersecurity dilemma which generates less predictability, prosperity, and cybersecurity, but rather the other way around: an inadequate level of cybersecurity – too weak or too strong – causes the initiation and the rise of the cybersecurity dilemma. In fact, one of the preliminary remarks of the second

[7] George Cristian Maior (coord.), *Un război al minții: Intelligence, servicii de informații și cunoaștere strategică în secolul XXI,* Bucureşti, Editura RAO, 2010, pp. 58-59.

chapter is that the cybersecurity dilemma is an effect rather than a cause of the weak governance of cyberspace.

I couldn't exactly determine whether the cyber power hierarchies follow closely the other ones from the land, air, sea, and space domains. However, I have validated the theories according to which most of the international actors can engage freely in challenging the others cyber power, without the power hierarchies from other strategic domains being crucial in that sense. From this perspective I have shown that there are enough reasons according to which the study of cyber geopolitics might become more significant during the next years.

Concerning the application of international law in cyberspace, I have analyzed which are the most important hurdles in preventing and fighting the factors which may contribute to the initiation and escalation of the cybersecurity dilemma. Unlike the reality expressed by most authors – not necessarily exact, but unlikely – I have underlined the reasons for which I do not believe that we are witnessing a lack of legislation, but rather a deficit of relevant international jurisprudence. Last but not least, I have identified the main reasons for which I strongly believe that protecting the fundamental rights and liberties of users and non-combatants in cyberspace must be superior to other principles of international law, in particular when dealing with the legitimate use of cyber force.

To synthesize: in the second chapter I have coined my personal view on the cybersecurity dilemma. Although I agree that cyber operations have a vital role within joint forces operations, from the perspective of a security dilemma I have proven that their power to replace the traditional weaponry is still limited.

3rd Chapter

As Robert Cooper stated that *the 21st century might be hijacked […] by anarchy and technology*[8], in the third chapter I have checked whether good governance really does have a significant contribution to the peaceful resolution of the cybersecurity dilemma.

Contrary to my initial expectations, I have observed that the reasons for which the cyberspace actors opt-in for good governance are not very diverse. I have noticed that good governance is not primordial for the competitive actors of cyberspace. Most of the time, competitive actors opt-in for pseudo-good governance behavior, in the sense that not rarely

[8] Robert Cooper, *Destrămarea națiunilor: Ordine și haos în secolul XXI*, București, Univers Enciclopedic, 2007, prefață, p. fn.

their good governance commitments are neglected “when necessary”, as they may prove an obstacle in protecting their own interests. However, in the case of second-rank actors the desire for action (the bandwagoning effect) tends to be more visible, for the simple reason that good governance might protect them against the hegemonic behavior of the more powerful competitive actors.

Without claiming an ideal solution, in the third chapter I have argued the significant contribution of good governance to the peaceful resolution of the cybersecurity dilemma. While identifying the fundamental principles of good cyberspace governance I had in mind that cyberspace does not lack strict rules on how international actors should behave, but rather needs more good governance in order to reach an optimal level of security, freedom (liberties), and prosperity. Therefore, for the peaceful resolution of the dilemma, I suggest that the security, freedom, and prosperity in cyberspace should be universally recognized as fundamental rights of individuals as soon as possible. To reach this, I have (indirectly) argued the need for adopting an internationally recognized “Good cyberspace governance charter, for protecting the cyberspace future against the effects of the cybersecurity dilemma.

One of the main conclusions of the third chapter is that good governance contributes to the peaceful resolution of the cybersecurity dilemma. I argued that the optimum of cyberspace sustainable development may be reached only when there is an easily identifiable analogy between security, freedom (civil liberties), and prosperity. As a first step towards good cyberspace governance, I have argued in favor of public-private CYBERINT collection agencies as means against violating transparency, rule-of-law, and civil liberties. Moreover I observed that information classification exigencies may not necessarily be an obstacle for the implementation of the good governance, neither the free circulation of data and information through cyberspace. Despite the possible criticism, I decided to open the academic debate in the sense of studying the manner in which dissident actors (or actors with a dissident potential) towards good cyberspace governance may be involved in assuring the sustainable development of cyberspace. For the time being, I have identified certain arguments which lead me to believe the advantages may be significant in that sense.

4th Chapter

Given that I have identified significant arguments to back the high consistency of the general hypothesis, in chapter four I have resorted to a case study to exemplify in a practical fashion the interdependence between Romania's cybersecurity and the quality of its national cyberspace governance. I have chosen to analyze the case of Romania because I consider it a good and appropriate opportunity to verify the results of my research. Also, I wanted to draw attention to the fact that researching the interdependencies between Romania's level of cybersecurity and the quality of it's cyberspace governance is quasi-non-existent, despite the expectations.

In brief, I obtained valuable clues according to which the "traditional patterns" of governance specific to other strategic domains may be harmful for the durable development of cyberspace. For starters, at least when it comes to transparency, cooperation and national security, I have noticed that the "traditional patterns" of governance have proven to have a doubtful efficiency in time and have increased the skepticism of Romanian users towards the national security needs in cyberspace, sometimes even reaching self-radicalization.

Despite my initial expectations, the discrepancies found regarding the security and governance of the Romanian cyberspace are not very alarming. However, I have noticed that the progresses made by Romania ever since joining transatlantic organizations are important indeed, but yet insufficient for reaching the optimum of security, freedom, and prosperity in the same time.

As regarding Romanian national cybersecurity, I have remarked that Romania is not very different from other countries alike within Europe. In that sense, I have appreciated as a positive development the fact that Romania did not engage in clandestine mass surveillance (in)security spirals and cybersecurity dilemma recently.

Summary of the conclusions

As a whole, the current thesis reveals solid grounds according to which cybersecurity strongly relies on (good) cyberspace governance.

Contrary to my initial skepticism, the general hypothesis is confirmed, as well as the fact that the cybersecurity dilemma shows up in cyberspace as well, though in a particular form. My research refutes the hypothesis according to which good governance

plays a very limited role in the peaceful resolution of cybersecurity dilemma and durable development of cyberspace as well.

Keywords: cybersecurity, good governance, cybersecurity dilemma, cyberspace, cyber-threats