# THE UNBEARABLE LIGHTNESS OF CYBER:

# CYBERSPACE AND STATE SOVEREIGNTY

MURAT CAN

BOĞAZİÇİ UNIVERSITY

2016

# THE UNBEARABLE LIGHTNESS OF CYBER:

# CYBERSPACE AND STATE SOVEREIGNTY

Thesis submitted to the

Institute for Graduate Studies in Social Sciences

in partial fulfillment of the requirements for the degree of

Master of Arts

in

Political Science and International Relations

by

Murat Can

Boğaziçi University

2016

DECLARATION OF ORIGINALITY

I, Murat Can, certify that

- I am the sole author of this thesis and that I have fully acknowledged and documented in my thesis all sources of ideas and words, including digital resources, which have been produced or published by another person or institution;
- this thesis contains no material that has been submitted or accepted for a degree or diploma in any other educational institution;
- this is a true copy of the thesis approved by my advisor and thesis committee at Boğaziçi University, including final revisions required by them.

Signature .....

Date 26.09.2016

ABSTRACT

The Unbearable Lightness of Cyber:

Cyberspace and State Sovereignty

This thesis explores the relationship between the cyberspace, which has turned into an inseparable part of individual and social life in every way imaginable and state sovereignty, a fundamental concept of the political science and it attempts to analyze and reveal what implications this new domain called cyberspace can hold for the nation-states. After first delving into what the concepts cyberspace and sovereignty are, the thesis explores the existing literature on cyberspace and state sovereignty. The case studies, which support and depict the main argument of the thesis, are presented under subtitles in a single chapter, constituting the primary section of the thesis. The same chapter also moves on to listing the technical features of cyberspace, both physical and non-physical, that hold significance and potential for the nation states. The thesis ultimately argues that, rather than simply strengthening or weakening state sovereignty, the cyberspace, by deepening and diversifying the interaction channels between the state and other states and non-state actors, both strengthens some aspects and practices of sovereignty and erodes some other aspects of it. The concept of sovereignty needs novel definitions and contemplations in the contemporary era due to the challenges such as cyberspace.

# ÖZET

## Siberalanın Dayanılmaz Hafifliği:
## Siberalan ve Devlet Egemenliği

Bu tez, son yıllarda insan ve toplum hayatının her açıdan ayrılmaz bir parçası haline gelen siberalan ile siyaset biliminin en temel kavramlarından biri olan devlet egemenliği ilişkisini incelemekte ve siberalanın ulus devletler için ne tür etkileri olabileceğini incelemeye ve göstermeye çalışmaktadır. İlk olarak siberalan ve egemenlik kavramlarının ne olduğu gözden geçirilmiş ve siberalan ile devlet egemenliği üzerine yazılmış literatür incelenmiştir. Daha sonra, tezin asıl iddiasını gösteren vaka analizleri, tezin ana kısmını oluşturan bir bölümde altbölümler halinde değerlendirilmiştir. Bu bölümde ayrıca, hem fiziksel hem de yazılımsal açıdan siberalanın ulus devletler ve devlet dışı aktörler için önem arz eden özellikleri sıralanmıştır. Tez nihai olarak siberalanın devlet egemenliğini sadece güçlendirmek ya da zayıflatmak yerine, bir devlet ile diğer devletler ve devlet dışı aktörler arasındaki ilişki kanallarını genişleterek bu ilişkileri derinleştirmekte ve çeşitlendirmekte olduğunu öne sürmektedir. Bu şekilde siberalan, devlet egemenliğinin kimi yönlerini ve pratiklerini güçlendirirken, kimilerini de oldukça aşındırmaktadır. Günümüzde siberalan gibi bir çok teknolojik gelişmenin sınamasına maruz kalan egemenlik kavramı, yeni tanımlamalara ve gözden geçirmelere ihtiyaç duymaktadır.

## ACKNOWLEDGMENTS

"There are things that you can't do – like writing letters to a part of yourself. To your feet or hair. Or heart." Arundhati Roy, *The God of Small Things*

Some things, however, are absolutely possible to do, like writing this thesis. But even this humble attempt required some indispensible and invaluable people to whom I should specifically pay homage in name and offer my non-cyberspatial thanks. I wholeheartedly thank my sweet and helpful thesis advisor Assist. Prof. Gül Sosay, without whom both this thesis and my MA degree would simply be non-existent. She guided me through all the processes with extraordinary energy, boundless patience and evergreen care. My two other thesis committee members, Assist. Prof. Zühre Aksoy and Prof. Asım Karaömerlioğlu enriched my thesis with their precious guidelines, and their participation in the thesis committee.

My precious friends, the lights of my eyes, namely, Oğuzhan Dursun, Aysun Kale, Ahmet Tekin, Yakup Öztürk, Emre Uzundağ, Oğuzhan Mamaşlı, Yasin Taşdemir and Pınar Yüksel should also be thanked here in name. I should not try to find any words to describe their friendship, for that would merely be confining it to soulless words. My mum and my dad, without whom I would not have any degree at all in my life, deserve the greatest credit.

Two green eyes, which followed me from Cairo to Berlin, from Washington DC to Belgrade, from London to Damascus, from Nashville to Sarajevo, from Warsaw to my military service in the Air Corps, need to be mentioned here as well, for they not only enriched my life with terre verte colored hues, but also introduced meaning to it once and for all. I realized very lately that it happens once in a lifetime and when it happens, it is enough.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

# CHAPTER 1

# INTRODUCTION

"By God! This is the end of diplomacy!" exclaimed Lord Palmerston, then the British Foreign Minister, upon receiving his first telegram in the 1840s. The following years showed that his worries were not rightful and, not only the telegram but also all the technological communication inventions turned into efficient apparatuses of the diplomacy and the state mechanism, rendering both even more effective. In a similar way, all the communication technologies that followed the telegram in the following centuries all brought up discussions regarding their political implications and whether they are going to lead to any change in the nature of polities or not. The television, the landline telephone and the GSM technology were all discussed in the same vein, if not as the forbearers of a revolution.

A similar debate followed the advent of the cyberspace, after it was quite apparent that, towards the end of the 1980s, the TCP/IP network, basically a technology that made it possible for distinct computers and devices to communicate over a common protocol system, was going to be the way how the communication would be in the following decades and centuries. The primitive form of this network was first a system developed to be a communicative platform between only a couple of government (and university) circle computers. However, this network soon turned into a giant global network to which all other networks connected and it came to be called with another popular name: the Internet. This network was now home to a virtual space of its own, with its own form of existence, a different logic of time, space, memory, reality and such. Cyberspace was, and still is, hard to define for anyone, especially for those not familiar with it, since it did not reside within any

borders of the nation states, but was not entirely detached from the real physical space, either. It was above and beyond human reality, but was also narrowed or enlarged horizontally and vertically by human factor.

These characteristics – above all the fact that it does not reside within a single country's borders, or on physical ground – all make cyberspace a drastically different technology from all other predecessor technologies. It definitely has political as well as social implications for the social life, political processes, and most significantly, the core of the nation state idea: sovereignty. The reason for this is that cyberspace, unlike any other previous technological advances, is unique in that it does not reside physically in the actual ground and constitutes a platform where each actor, political or not, can easily perform an existence. While the classical sovereignty was, and still is, exercised on the real space, within clearly defined boundaries and on actual soil (or water and air), the virtuality of the cyberspace makes it difficult for nation states to exercise such a classical sovereignty on. Besides this, however, similar nation state borders are also perfectly drawn in the cyberspace at the same time, such as those of Russia, China and North Korea, which restrict and control the cyber movements in and out. The lives of individuals and non-state actors are closely monitored and controlled to an extent unprecedented in the human history, due to the very fact that the actions on cyberspace can be easily tracked through various methods. Yet another fact is that non-state actors are also unprecedentedly powerful against the nation-states due to the very fact that anything can be instantly shared and distributed thanks to cyberspace in seconds, which would otherwise take days or weeks.

Another factor is that the cyberspace offers a degree of anonymity, if properly employed, to its users, which guards the non-state actors (and sometimes the states

themselves) against being detected and convicted. These brief examples all make one think about the dawn of a novel way of exercising and confronting state sovereignty. What is the condition of sovereignty, a concept almost as old as the social existence on earth, challenged by the dynamics of cyberspace? Are social sciences involved in cyberspace studies as much as they should be? Is cyberspace a platform that strengthens or weakens the state sovereignty, given the enormous complexity of the actors and relations within it? Or, rather than these direct and simple outcomes, does it promise subtler and more complex changes for political and social world? This thesis is a humble and short yet significant attempt at trying to come up with accurate answers to such questions, within the discipline of political science.

In addition to these characteristics of cyberspace that make it unique for state sovereignty, maybe the greatest characteristic of the cyberspace is the incredible amount of speed that it offers. It can be argued that the speed of the cyberspace poses the greatest challenge for the abilities of states to exercise their sovereign powers. The only way for states to keep their sovereignty from getting eroded is using the cyberspace speed themselves before any other actor can effectively do so, but this is not always the case. Social mobilization against a state, trading without the control mechanism of a state, travelling or communicating without the approval of a state are all possible within seconds now, and this might be the greatest challenge a nation state can ever imagine.

All these characteristics make cyberspace a fertile ground for social science research. However, the existing research regarding the cyberspace is mostly about the technical side of it, quite naturally so, since almost all researchers regarding cyberspace come from engineering and other technical fields, though cyberspace is a phenomenon that affects almost anyone. The social sciences seem a bit late in

including the cyberspace factor into their research, partly due to the unfamiliarity of such an alien topic and partly due to a lack of experience as to how to conduct research in such a newly-born area. There are surely many research works that are directly and indirectly on cyberspace, both in the forms of books or articles. Yet, firstly, they are so little and insignificant in terms of their number and scope that they mostly go unmentioned and unnoticed. Secondly, they seem to be stuck in a dichotomy that shaped the 1990s' political science landscape, and thus they mostly either simply claim that cyberspace strengthens or weakens the state sovereignty. Thirdly, and more importantly, they are too outdated in that they naturally fail to incorporate the advances in the use of cyberspace in political or social world after the 2000s and especially the 2010s. The hacking scandals, technical features of cyberspace that allow the states to monitor their citizens, the rise and use of social media in the mobilization of the street protests around the world were all lacking in the research on cyberspace, and even when they were not lacking, they were not given the due attention and focus.

This present thesis is an attempt to fill such a void in the literature by both considering the latest advances in the cyberspace and trying to come up with a more profound analysis than the ones preceding it. It is exclusively significant in the sense that it revisits and updates an important political science debate that was left in the 1990s and has been untouched ever since. By looking at the most recent technical features and uses of the cyberspace by state and non-state actors, the thesis brings about an old unresolved discussion to the fore, and comes up with a more sound and more grounded main argument, which also creates a potential for further future research on the topic.

The main argument of this thesis is that the cyberspace, rather than simply strengthening or eroding the state sovereignty, does both, and thus changes the geometry of the sovereignty by altering the outlook of the relations between the state and non-state actors and other states. This is not a zero-sum game as the previous researchers chose to look at the subject. The state is even stronger vis-à-vis the individuals and non-state actors, quite stronger than the absolutist states, but non-state actors are also stronger vis-à-vis the state, since they are able to challenge the state in a whole new set of ways. Cyberspace can thus never be fully understood if it is viewed merely as a regular tool that is at the hands of either party. It can be fully understood and analyzed only when it is viewed as a newly-opened battle field where the opponent parties (if they are opponents at all) are on the fight with even stronger capabilities than their previous battles. Cyberspace increases the interaction channels between these actors and grants them with novel capabilities. In the end, rather than only one actor being simply more capable, strong, "sovereign", more challenging and more reckless, both parties get sometimes different and sometimes similar kind of strengths and tools to check and balance the other. This can be summarized as the cyberspace, rather than simply strengthening or weakening state sovereignty, it deepens and diversifies the interaction channels between the state, other states and non-state actors and brings about a whole new geometry of sovereignty, which is the main argument of the thesis. The interaction points and scopes between the two actors now are many more than the previous ones, which requires deeper, more detailed studies in the future.

While putting forward its main argument, the method this thesis employs is the case study method. The case study method is the most suitable one for the purposes of such a thesis since "case studies are pertinent when your research addresses either

a descriptive question or an explanatory question" (Yin, 1993, p. 5). The research question of the thesis requires a method which can reveal in-depth results of how a phenomenon can be, and is, altered through the extensive use of another factor and case study thus seems a logical option, rather than a simple survey or statistical comparison of the available data. The cases selected for the purpose are the ones that include a depictive side of the use of cyberspace relevant to the sovereignty of a specific state. They are not simple hacking (or any other use of cyberspace) incidents that have only technical value, but are the ones that hold meaning and implications for the discipline of political science in general and they all involve an example of strengthening or eroding state sovereignty for the state in question. All in all, these cases ultimately demonstrate that the state sovereignty is both strengthened and eroded in various incidents, as the power of the non-state actors vis-à-vis the state mechanism is. The number of cases is 8, as the result of long and illuminating debates with my advisors and they all more or less clearly depict a different side (and use) of cyberspace showing its either strengthening or eroding features for the state sovereignty.

The thesis is organized in 6 chapters and develops step by step towards achieving its main purpose. While the first chapters try to clear the way for the main middle chapters by attempting to explain the two main concepts of the thesis, namely, the cyberspace and the state sovereignty, the middle chapters deal directly with the political science argument of the thesis. One of them is an extensive literature review and the other one is the main core of the thesis (case studies). The last chapter is the one that concludes the thesis and suggests further research on the topic. The thesis thus develops as follows:

Chapter 1 is the Introduction, and as its name might suggest, is an introductory chapter to the thesis. It includes the main argument of the thesis, together with the method, scope and purpose of it. The gap in the relevant literature that the thesis is expected to fill is pretty briefly discussed (it is handled in detail in the Chapter 4, the main literature review chapter) and the significance of the thesis is put forward. It also shows the organization and development of the thesis, together with its strengths and weaknesses, in order to guide the reader and prepare them for a better following.

Chapter 2 is a chapter that tries to familiarize the reader with the concept of cyberspace. Bearing the title "The Geography of Cyberspace", it combines together the available definitions and explanations of this concept. The technical definitions and social science definitions of "cyberspace" are reviewed under two distinct subtitles accordingly, and the history of the cyberspace is revisited. While writing its history, how it technically developed from its initial stages and how it came to such a vital central position in the modern world are included. The chapter also analyzes how and in which social science disciplines the cyberspace has been handled. Though the chapter might sound alien to the social scientists and flawed and insufficient to the technical scientists, such a thesis required exactly this kind of a chapter, which succinctly introduces a new technical concept without drowning the readers with redundant technical information. The chapter specifies which cyberspace definition is relevant for this present thesis and how to approach it appropriately, in a way that prepares the reader for what to follow.

Chapter 3 has the title "The Concept Sovereignty" and it attempts to compile the definitions and historical understandings of the concept "sovereignty" and determine one of them, one that is extensive and practical enough to work with, as the sovereignty definition to be used throughout the thesis. The chapter also deals

with the recent theoretical works regarding the sovereignty, as well as the debates in the last decades regarding whether sovereignty is a concept that is at the trend of eroding or strengthening as a result of the immense technological advances, globalization, capital flows, migration and democratization. Besides going through all these theoretical angles of sovereignty, the chapter also operationalizes the most appropriate sovereignty definition to render it easy to work with. The chapter generally tries to clarify very basic yet ambiguously debated political science concept, just as the previous chapter did regarding another concept.

Chapter 4 is "The Relationship of Cyberspace and Sovereignty" and this chapter is a quite dense, long and extensive chapter since it is the main literature review of the thesis. It reviews all the literature written on the relationship between the cyberspace and the state sovereignty starting from the first articles onwards and it tries to simplify this literature by dividing all such works into two camps: the ones that argue that cyberspace is (or will be) a factor that erodes the state sovereignty as we know it and the ones arguing that it will be a tool of the governments, helping them consolidate their sovereignty even more. The literature is surely more diverse and detailed and it is thus hard to be packed into simply two dichotomic categories; however, to make it conveniently understandable, the chapter uses these two subcategories. The relative strengths and weaknesses of the works reviewed are also included, if they have any, together with the context in which these works were written or conducted. The chapter constitutes a real bridge to the subsequent one by linking both the previous definitional chapters and the earlier literature works to the main argument of the thesis.

Chapter 5 is the one that constitutes the backbone and the core of the thesis, in that, it is the one in which case studies are stated and analyzed. It has the title of

"Case Studies: Sovereignty Strengthened, Sovereignty Eroded" and composes of eight different cases where the use and abuse of the cyberspace had a visible political/social effect on the concept of sovereignty. The cases were selected not only because they had such a vast effect but also they have explanatory power for the purposes at hand. One point to note about this chapter is that, the cases selected seem to come from a wide array of sources, both state and non-state actors, sometimes even individuals, but ultimately they all have some sort of an influence on the sovereignty of a state. The reason of this diversity of the sources of the incidents in the cases is simply the cyberspace's unique characteristic that allows for the presence of all kinds of actors within it. The cases selected are Bitcoin, 2014 Russian Dominance of Ukrainian cyberspace, Stuxnet, the Egyptian Revolution of 2011, 2014 Sony Pictures Entertainment Hack, the various hacking activities of the RedHack group, China's Firewall and the NSA cyber practices (as revealed by the Snowden Case). Each case is analyzed under a relevant subtitle, together with its brief history, process, direct or indirect implications for the sovereignty of a state, and the evidences revealing in what ways the sovereignty took shape as a result of the use of cyberspace. The chapter basically aims to reveal the main argument of the thesis to the reader through actual empirical case examples from a quite recent history. This chapter also includes a part where some technical features and advances in the cyberspace that have the potential to have political significance for the sovereignty of nation states are discussed. They do not necessarily correspond to specific incidents (as the empirical cases previously do) but are only listed-down technical advances and features that cyberspace offers. This is significant in the sense that it might lead to further research regarding the subject and furthermore, and without such a part, the thesis would be quite incomplete.

The last chapter, Chapter 6, is naturally the conclusion chapter and it concludes the findings of the thesis as a whole and puts everything briefly in a concluding summary.

The name of the thesis, "Unbearable Lightness of Cyber: Cyberspace and State Sovereignty," is a clear reference to the book by the Czech author Milan Kundera, and it arguably reflects the elusive, abstract, misty nature of cyberspace and its quite powerful, heavy and must-be-considered presence. It seemed to me the most suitable and meaningful title for such a thesis.

After these general introductory notes on the thesis, the strengths and weaknesses of the thesis must be noted down here as well, so that the readers know what they are holding. As for the strengths of the thesis, it must be firstly noted that it is one of the unique works since the cyberspace is not a subject that is extensively studied or written on, despite its extremely wide usage in the modern world. When the cyberspace is studied, it is done so only by the cyber security engineers and the subject of their study is almost always codes, networks and such, rather than the political/social significance of the cyberspace. And when social scientists study cyberspace, they either focus on its usage in the mobilization of masses in street protests (as did many researchers regarding the use of social media during the Arab Spring) or they focus on the cyber capabilities of the state militaries around the world, which is more in the International Relations tradition rather than that of the political science. This thesis takes one ontological step back and rather than focusing on merely one use of cyberspace, approaches it as a whole. Secondly, the political science works on cyberspace are mostly stuck in the 1980s and 1990s, the time when the cyberspace was only fledgling and had only a few webpages. They thus base themselves on predictions about the future usage of the cyberspace rather than

empirical findings. This thesis is aware of the advances in 2000s and especially the 2010s and includes them in its analyses. The developments in the 2010s, as the case studies quite clearly reveal, embody the political and social potential of the cyberspace. Thirdly, one another strength of the present thesis is that, it tries to simplify its arguments and points, so that the reader, even though he/she has no previous technical knowledge of the area, might picture everything in his/her mind. The main argument of the thesis is specifically simplified and in such a way, besides updating the cyber-political literature scattered into last two decades, it offers a reader-friendly reading experience.

As for the weaknesses of the thesis, it must admittedly be noted that the thesis, for the reasons of academic convenience, might at times oversimplify the complex phenomena. The most significant oversimplification is that, whether a cyberspace technique strengthens or erodes state sovereignty is mostly related to the regime and governing principles of a state in question. A cyberspace feature such as a network firewall or web censoring might be a powerful tool that strengthens the hand of an authoritarian state, while it might be of no use for a liberal democratic state which values the freedom of speech. Social media, for instance, is used not only by the masses and non-state actors (which is supposed to make us think that social media is inherently a phenomenon that might erode state sovereignty,) but it is also widely used by states themselves as propaganda platforms in ways that add up more strength to their internal and external sovereignty. Cyberspace features are mostly used by both parties. Even hacking, which one might expect to be illegal and thus used only by criminal-minded non-state actors, is used by the very states themselves, as the Stuxnet case showed in 2010. The cases and judgments in this thesis, therefore, ignore these convoluted cyberspace relations and oversimplify what would normally

be extremely complex. The oversimplification, though it is a weakness, should not be understood as a serious flaw, because only through such a basic introductory way can we study cyberspace in the scope of an MA thesis. However, it should be noted that further future studies should take into consideration the regime factor as an independent variable and look at the results accordingly. The democratization and liberalization processes are key to understanding the political and social significance of cyberspace. It should be noted that even my decision to ignore regime as a variable and focus on "state" only, can be interpreted as an indicator that the present thesis is more within the realist camp. It is partially true, but the realist perspective is not deliberately adopted but rather, the way the thesis tries to analyze the cases in a simple and succinct way brings the thesis to such a point. The author of the thesis is aware of this fact, and believes that further studies on cyberspace with more detailed theoretical background will take into account regimes, cultural variables, economic indicators, geographical tendencies and such while studying cyberspace and will come up with more sound conclusions.

Another weakness of the thesis stems from the fact that it was written by an aspiring social scientist writing about a technical subject. Though it is about its social side, it might include some drawbacks at times. This is a necessary nuisance since an engineer's or a technical scientist's take on a political subject would also be flawed, perhaps more than this present thesis. These weaknesses expressed here do not violate the thesis's importance and its claim to fill a significant gap in the literature. If it does not live up to its claim, it might at least constitute an introductory work for those who plan to conduct further research on social-cyber issues.

This introduction chapter aimed to introduce the reader to what is to follow in the further chapters. After briefly looking at the purpose, method, significance,

organization, strengths and weaknesses of the thesis, it is now appropriate to move on to the second chapter which is a detailed and extensive text about the concept of cyberspace.

# CHAPTER 2

# THE GEOGRAPHY OF CYBERSPACE

"Jacques: I do not like her name.
Orlando: There was no thought of pleasing you when she was christened."
Such are the lines of Shakespeare in one of his plays regarding the name of another character, which would, I guess, be the most suitable epithet for any study regarding the concept of cyberspace. It is an elusive concept that does defy easy defining and one on whose definition, categorization and classification many ideas differ. Though almost everyone uses the term nowadays since the cyberspace is now an indispensible feature of human lives, the answer to what cyberspace is, is not so easy to give. In one of the episodes of the British TV Series *The IT Crowd*, one of the characters shows a small black box to a newbie IT member and says "This is the Internet," after which, the newbie boosts to have seen "the source of the Internet as we know it" throughout the episode.

What is cyberspace, then? Is it the wires, the physical devices that are employed to connect to the cyberspace, the virtual world consisting of the webpages and information, or is it all these combined?

The term "cyberspace" is hard to describe and define, primarily because it is both hard to visualize and impossible to physically locate. This difficulty regarding cyberspace, and the technological terms in general, have led social scientists to abstain from analyzing these concepts from their disciplines' points of views and caused these kind of analyses to be marginal in the great literature of social sciences up until the recent years. The central role that cyber domain has come to play in all

the aspects of human lives, however, resulted in a fresh interest in cyberspace among social scientists. The definition and description problem that posed a predicament for social scientists did not really matter for technical scientists and engineers, since they delved into studying systems and codes without feeling the need for definitional clarity of the term. The cyberspace, however, and the geography, if any, thereof, need to be clarified for social scientific analyses, such as this thesis.

The problem with defining what cyberspace is, let alone its characteristics, lies with the fact that it emerged both recently and is "virtual" in every sense of the word. Weinberger (2002), in his book primarily devoted to cyberspace, suggests

> The Web, […] has no geography, no landscape. It has no distance. It has nothing natural in it. It has few rules of behavior and fewer lines of authority. Common sense doesn't hold there, and uncommon sense hasn't yet emerged. […] We don't yet even know how to talk about a place that has no soil, no boundaries, no near, no far. (pp. 8-9)

The difficulty also partly stems from the fact that cyberspace, unlike other technological advances, poses a chaotic, anarchical and elusive platform. In the words of Post (2009), "Jefferson biographer Joseph Ellis called cyberspace 'the perfect Jeffersonian environment,' all decentralization and disorder, growth and expansion, a frontier that is constantly expanding and seemingly illimitable" (p. 117).

The definitions of cyberspace, though vague in nature, all resemble each other more or less, focusing on the virtual "space" created by computer networks and where these interactions take place. Though they look somewhat similar, their focus tends to be either technical or social-science-oriented, depending on by whom or for whom they are written. This chapter firstly compiles the social science-related cyberspace definitions, since they are longer and more relevant for the thesis. The technical definitions are also collected under another subtitle. After these definitions,

another subtitle puts forward and explains the cyberspace definition which is going to be used throughout the entire thesis, namely, that of David Clark. The chapter then presents a brief history of the cyberspace up to the point of how it came to the center of the modern human life. After this, the place and context of cyberspace in social science are generally reviewed in order to have a look at how it has been approached by the social scientists.

## 2.1 Cyberspace defined by social scientists

It is no wonder that the cyberspace definitions by the social scientists are more understandable and more reader-friendly, since the redundant technical details are dropped out in these definitions. The dictionary definitions of cyberspace aside (which are more or less the same,) this part attempts to compile the definitions of cyberspace by social scientists. Post (2009), in his book, which attempts to explain the cyberspace to social scientists, argues that the cyberspace is, at the bottom line, the network, which reminds one of the simplistic dictionary definitions:

> We need to be a little clearer about what it is we are calling "cyberspace" in order to provide one. Whatever else it may be, cyberspace is, at bottom, just a network linking computers together so that information, in the form of electronic pulses (on/off, one/zero), can be transmitted from one to another. There are thousands upon thousands of such networks out there—millions, probably, by now: local area networks (LANs), wide area networks (WANs), home networks, office networks, interoffice networks, wireless networks, intranets, extranets. (pp. 24-5)

These all networks, whether closed or open, whether small or large, are all parts of what is called the cyberspace. "The big one is known as *the* inter-network, or, more simply, the Internet" (Post, 2009, p. 24-25). This largest network is now, basically, what we come to call as cyberspace.

As the cyberspace was discovered to be a politically significant domain that is somehow relevant for the international politics, the states got involved in drafting cyber security policies and action plans which also had novel, more comprehensive cyberspace definitions, since the earlier dictionary definitions did not suffice any longer. One such definition, which attempted to focus on the political and national importance of cyberspace, was offered by the action strategy of the White House in 2003. It defined cyberspace as "the nervous system—the control system of our country […] composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infrastructures to work" (US Department of Homeland Security, 2003). This definition, rather than focusing on the spatial characteristics of cyberspace, defined it more as a network on which the critical infrastructure of the country is managed. The use of "our" in the definition renders it more of a US-specific national action plan definition rather than a generic definition for the general use of cyberspace. However, this definition holds significance firstly because it was a first out-of-dictionary entry, and secondly because the importance of cyberspace for politics was recognized through it.

A few years later, yet another political US document defined cyberspace as the following: "Cyberspace is a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify and exchange information via networked information systems and physical infrastructures" (Department of Defense, 2006). This definition included a leap forwards since it made use of the term "domain," considering cyberspace as a "space" whose security should be defended just as that of the sea or airspace. This spatial focus, however, was dropped in another cyberspace definition by another US institution, namely the Homeland Security. According to this 2008 definition, cyberspace is "the interdependent network of

information technology infrastructures, and includes the Internet, telecommunication networks, computer systems, and embedded processors and controllers in critical industries" (Homeland Security Presidential Directive, 2008). Since this definition was drafted in a national document as well, which was written in a very specific context, the main focus was the safety and security of information networks on which the government was dependent. The cyberspace, therefore, was not defined as a space or domain. A similar network and structure-based cyberspace definition was offered by Gordon England, during his office in the Department of Defense. England (2009) defined cyberspace as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunication networks, computer systems, and embedded processors and controllers."

Although most of the definitions employ some technical-sounding aspects of cyberspace, these definitions are all put forward *by* social scientists, *for* social scientists. It can be seen from the definitions that cyberspace is mostly conceived as the network that is formed when computers are linked together, which is, what cyberspace basically is. However, a virtual space is also produced when the network communication is provided, which is more than just the network components between the computers. Some definitions highlight this aspect of cyberspace that seems to be slightly ignored in most of the definitions. Don Slater (2002), for instance, describes cyberspace with a metaphor: "sense of a social setting that exists purely within a space of representation and communication […] it exists entirely within a computer space, distributed across increasingly complex and fluid networks" (Crofton, 2015, p. 85). It is true that there is no physical space where all the information in cyberspace is located and the network consists basically of a

computer that demands cyber information from another computer that serves the information that is demanded. So when a user's computer or tablet connects to cyberspace to enter a website, it is merely connected to another server computer located elsewhere. However, a space can be argued to come into existence due to the very nature of this connection. While cyberspace should not be confused with the Internet, the term is often used to refer to objects and identities that exist largely within the communication network itself, so that a website, for example, might be metaphorically said to "exist in cyberspace." According to this kind of approach, events taking place on the Internet are not happening in the locations where participants or servers are physically located, but "in cyberspace." Bruce Sterling (1992) explains this somewhere in this book quite neatly:

> Cyberspace is the "place" where a telephone conversation appears to occur. Not inside your actual phone, the plastic device on your desk. Not inside the other person's phone, in some other city. The place between the phones. ... In the past twenty years, this electrical "space," which was once thin and dark and one-dimensional—little more than a narrow speaking-tube, stretching from phone to phone—has flung itself open like a gigantic jack-in-the-box. Light has flooded upon it, the eerie light of the glowing computer screen. This dark electric netherworld has become a vast flowering electronic landscape. Since the 1960s, the world of the telephone has cross-bred itself with computers and television, and though there is still no substance to cyberspace, nothing you can handle, it has a strange kind of physicality now. It makes good sense today to talk of cyberspace as a place all its own. (p 2)

The "space" metaphor in explaining the nature of cyberspace is debated between the experts. While some of them view this as necessary and helpful in explaining the cyberspace, "it has also been critiqued as being unhelpful for falsely employing a spatial metaphor to describe what is inherently a network" (Graham, 2013).

Kuehl, in his draft book regarding the strategic importance of cyberspace written as a textbook to be taught in the military higher education in the US, after analyzing quite many cyberspace definitions, finds a fault that inflicts all of them. He argues that these definitions fail to address the question "[W]hat makes cyberspace unique? If cyberspace is a domain alongside air, land, sea and outer space, what are its unique and defining physical characteristics?" (Kuehl, 2009). After he indicates this unanswered question, he claims to come up with the most comprehensive (and apparently, one that addresses the previously mentioned questions) cyberspace definition. For Kuehl (2009):

> [c]yberspace is an operational domain whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange and exploit information via interconnected information-communication technology (ICT) based systems and their associated infrastructures.

What Kuehl tries to demonstrate here as the unique characteristics of the cyberspace is that it is not given, and subject to the use of electronics and technology in general, in other words, the human factor, not the nature itself, unlike other domains. This finds its epitome in Lessig's words as the main characteristics of cyberspace, which can be basically summarized as the human intelligence behind its expansion and existence. Lessig argues that

> The architecture, the design, the constitution, the shape – these features that someone, some code writer, builds. This architecture makes cyberspace as it is, and this architecture can be different… The nature of this space is not determined by god; *the nature of this space is ours to set.* Whether one may travel in this space with the right of anonymity is a choice that we must make, not a choice that the nature of the space will assure. The space has the nature so that its code writers give it; yet we are the code writers, and we can do things differently. (Post, 2009, p. 210)

Although their focus often change, all of the cyberspace definitions above suggest that cyberspace is much more than the physical hardware that allows us to access cyberspace. Beyond the fiber cables, the computers, the modems, there is a "space," a domain and it has a geography. The word (or the term) domain is used plenty of times to denote the cyberspace. The dictionary definition of "domain" is "a field of action, thought, influence, the territory governed by a single ruler or government; realm, a realm or range of personal knowledge, responsibility, etc., a region characterized by a specific feature, type of growth or wildlife, etc." (Dictionary.com, 2015).

Akin to these definitions, the cyberspace is conceived by many to contain a space of its own, where the user enters to reach to the information such as webpages, which creates a sort of illusion that it has a territory of its own, directing researchers and enthusiasts to describe it as a domain. The word domain has also political significance, since it denotes the idea for users that it is a domain of a country and thus needs to be defended. This "space" emphasis on the cyberspace is contested though, and some scholars even reject that it is a domain. Yet, much of the existing literature, this thesis included, base their arguments on the notion that cyberspace exists as a space, however virtual and relative it might be. Now it is a generally accepted knowledge that "cyberspace [is] another domain of life, just as land, sea, and from the 20$^{th}$ century onwards, air" (Kuehl, 2009). For almost all analysts in the field, cyberspace is no different from these domains. Cyberspace has, in whichever way we choose to define it, come to a point on which all our social, political, economic, psychological, cultural and military activities are dependent. In the words of Kuehl (2009):

> The way that cyberspace has changed—some would argue is expanding astronomically—the ways that we can create, store, modify, exchange and exploit information has transformed how we operate in the other domains and use the instruments of national power. We can capture literally any kind of information—the human voice on a cell phone, the contours of a fingerprint, the contents of the Encyclopedia Britannica, or the colors of ice and dust as "seen" by a spacecraft on the planet Mars—store that information as a string of bits and bytes, modify it to suit our purposes, and then transmit it instantly to every corner of the globe.

Besides these compact definitions, the definitions of cyberspace by social scientists, as David Post's definition also exemplifies, make use of analogies as well. This helps the readers of their works understand the nature of the cyberspace, and these kind of analogies are unsurprisingly found only in the social science definitions, since technical scientists do not need or prefer any kind of simplification in their definitions. In one another analogy, the cyberspace is rendered as a similar physical space:

> A good analogy to help people understand cyberspace is to draw a parallel to your physical space. You are a person and you are somewhere; perhaps an office, house or at the car wash reading this on your iPhone. This is your environment, your space. You have objects around you that you interact with: a car, a sofa, a TV, a building. … Cyberspace is essentially the same: it is an environment in which you operate. Instead of physically "being" somewhere, you are using computing equipment to interact over a network and connect to other resources that give you information. Instead of "objects," like a car or a sofa, you have email, web sites, games and databases. (Martin-Vegue, 2015a)

Since the network nature of cyberspace has always been alien to the social scientists, the space-ness must have seemed a more studiable place for them, which is why this definition, together with others, made use of a space analogy.

The political and social significance of the cyberspace, once it was realized by the nation states, led them to come up with each state's own definition of cyberspace. As indicated above, the US was the first and foremost in drafting the first official cyberspace definition. The US official discourse focused more on the "domainness"

of the cyberspace, and the cyberspace's significant security role as the backbone of the national security, emphasizing that the critical infrastructure, such as dams, factories, airports, military bases and such are all functioned through the cyberspace. This characteristic of cyberspace led many other nation states to devise their own cyberspace definitions. While the official definition of the Turkish Republic describes the cyberspace as "the environment which consists of information systems that span across the world including the networks that interconnect these systems" (Open Technology Institute, 2015), focusing more on the space-ness of the cyberspace as previously told, the definition by the Netherlands is a more comprehensive one:

> For the purposes of this strategy, "cyberspace" is understood to cover all entities that are or may potentially be connected digitally. The domain includes permanent connections as well as temporary or local connections, and in all cases, relates in some way to the data (source code, information, etc) present in this domain. (Open Technology Institute, 2015)

The official Russian cyberspace definition also incorporates the human activity that many other descriptions ignored: "A sphere of activity within the information space, formed by a set of communication channels of the internet and other telecommunications networks, the technological infrastructure to ensure their functioning, and any form of human activity on them (individual, organizational, state)" (Open Technology Institute, 2015). The Russian definition unsurprisingly includes the activities of the state in the cyberspace definitions, a feature that is not commonly seen in other cyberspace definitions. It is no wonder, however, that the Russian definition included state activities as an integral part of the cyberspace definition given the immense number and impact of the Russian cyber activities,

backed directly or indirectly by the Russian state, as the case study chapter of the thesis shows in the related case.

The definition by Poland starts with mentioning the "spaceness" of the cyberspace but includes the relational component of it: "A space of processing and exchanging information created by the ICT systems, together with links between them and the relations with users" (Open Technology Institute, 2015). New Zealand definition, however, promotes cyberspace solely as a network and does not quite mention in any way the user interactions or the virtual space of the cyberspace, as other definitions do: "The global network of interdependent information technology infrastructures, telecommunications networks and computer processing systems in which online communication takes place" (Open Technology Institute, 2015). Latvia, quite affected by its cyber-aware neighbor Estonia, seems to have a more balanced and profound definition "Cyber space is an interactive environment that includes users, networks, computing technology, software, processes, information in transit or storage, applications, services, and systems that can be connected directly or indirectly to the Internet, telecommunications and computer networks. Cyber space has no physical borders" (Open Technology Institute, 2015). In addition, South African definition seems to be the best definition by a nation state: "Cyberspace means a physical and non-physical terrain created by and/or composed of some or all of the following; computers, computer systems, networks, and their computer programs, computer data, content data, traffic data, and users" (Open Technology Institute, 2015).

Now that the thesis has looked at how the cyberspace has been defined and approached in the social science literature, it is appropriate to look at how it has been handled in the technical literature.

## 2.2 Cyberspace defined by technical scientists

This brief subtitle reviews how the cyberspace is defined and described by the technical scientists, engineers and designers, the primary scientists that directly interacts with the technical structure of the cyberspace. Most of the definitions focus more on the "networkness" of the cyberspace, when they are put forward by technical scientists.

The network of cyberspace is a bit hard to visualize. There are various Internet maps that have been produced for various purposes. There have been some studies to visualize what cyberspace is, although it is basically impossible, as previously mentioned. The maps of the cyberspace for different purposes that have been created so far take into consideration the physical appearance of the Internet connections (in other words, the location of the people who connect to the Internet and the servers to which they connect,) or more popularly, the traffic of the Internet connections. The one most renowned cyberspace map is one that visualizes the large Internet network, ignoring the latest developments and complexities of the cyberspace, in order to give a basic idea of what it is. This map is shown in Figure 1 and is known as the "Peacock Map" since it resembles the elaborate tail of a peacock.

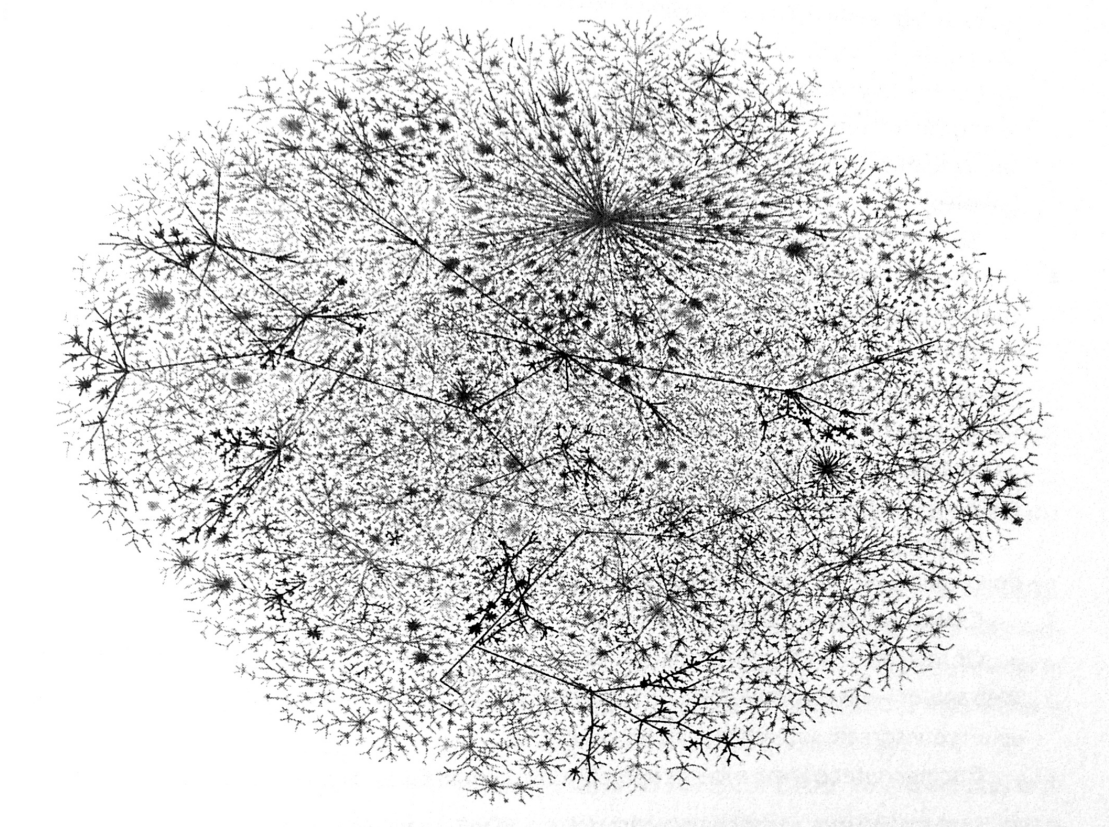

Fig. 1 The "Peacock Map" of the Internet (Source: The "Peacock Map" of the Internet, created by Hal Burch and Bill Cheswik, Courtesy of the Lumeta Corporation)

Technical definitions of cyberspace do not include other aspects of the phenomenon and define it just as a computer network. The definitions that can be classified as "technical" are almost always the definitions of networks and they more or less revolve around this following definition: "networked computing devices [that] exchange data with each other along network links (data connections). The connections between nodes are established using either cable media or wireless media" (Atis Telecom Glossary, 2016). When the issue of cyberspace is raised, the technical scientists tend to divide the network that they are talking about into its types, rather than having a holistic cyberspace definition. For instance, most of the definitions of cyberspace, when studied by technical scientists, include the following

information regarding the network (which is just one part of the cyberspace, according to social scientists):

> The smallest and simplest networks are local area networks (LANs), which extend over only a small area, typically within a single building or a part thereof. A home network is a type of LAN that is contained within a user's residence. Wide area networks (WANs) can extend over a large geographic area and are connected via the telephone network or radio waves. A metropolitan area network (MAN) is designed to serve a town or city, and a campus area network is designed to serve a university or other educational institution. (Linfo, 2005)

If one looks for a shorter and more succinct "network" definition than this long one by technical scientists, one encounters only another definition, and no more: "A computer network is a group of computer systems and other computing hardware devices that are linked together through communication channels to facilitate communication and resource-sharing among a wide range of users. Networks are commonly categorized based on their characteristics" (Technopedia, 2016).

After looking at both social science and technical science definitions of cyberspace, it can be safely argued that social science definitions focus on "spaceness" of the cyberspace, while technical definitions focus more on the "networkness" of cyberspace. This is quite understandable given the fact that each science tradition's epistemological outlook differs totally from one another. In addition to this wide difference, there seems to be one another difference between the early cyberspace definitions and the later ones. The early definitions, by their very nature, focus more on cyberspace's being a network, while the later definitions also include the human content of the cyberspace and the incredible amount of information data that is over the Internet, which makes the cyberspace feel more like a "space."

After having looked at enough number of cyberspace definitions, it is now appropriate to have a look at the cyberspace definition and model that will be used throughout this thesis. It must be noted that whenever the thesis mentions the word "cyberspace," it always refers to Clark's cyberspace model.

## 2.3 Clark's four-layer cyberspace model

After going through the cyberspace definitions and descriptions of both social and technical scientists, it is now the time to look at the cyberspace model that will be used in the thesis. The model (and therefore the definition) of cyberspace by David Clark (2010), stated in his study of cyberspace "Characterizing Cyberspace: Past, Present and Future" seems to be not only perfectly suitable for the purposes and scope of this thesis, but also it is the most comprehensible and organized cyberspace model, bringing together all the constituents of the phenomenon called cyberspace. The technical units such as modems, cables and computers, the information stored in the cyberspace such as websites, and the human users of cyberspace, all find a place in Clark's model as "layers" of cyberspace. This thesis, therefore, bases its arguments and findings on Clark's model, specifying at each point what "layer" of cyberspace is in question, where needed.

Clark's study conceives the cyberspace as consisting of four different layers. The first layer is "the physical layer" which means "the physical foundations that support the logical elements," (Clark, 2010, p.2) the physical elements of the cyberspace like nods, computers, cables, IXPs and modems that we use to connect to the cyberspace in the first place. The second layer is "the logical layer" and it is "the logical building blocks that make up the services and support the platform nature of cyberspace" (Clark, 2010, p. 2). The third layer is "the information layer," which refers to "the information that is stored, transmitted, and transformed in cyberspace"

(Clark, 2010, p.3). The fourth and last layer is “the human layer,” which is comprised of “the people who participate in the cyber-experience—who communicate, work with information, make decisions and carry out plans, and who themselves transform the nature of cyberspace by working with its component services and capabilities” (Clark, 2010, p.4). The four layers of Clark's model are seen in Figure 2.

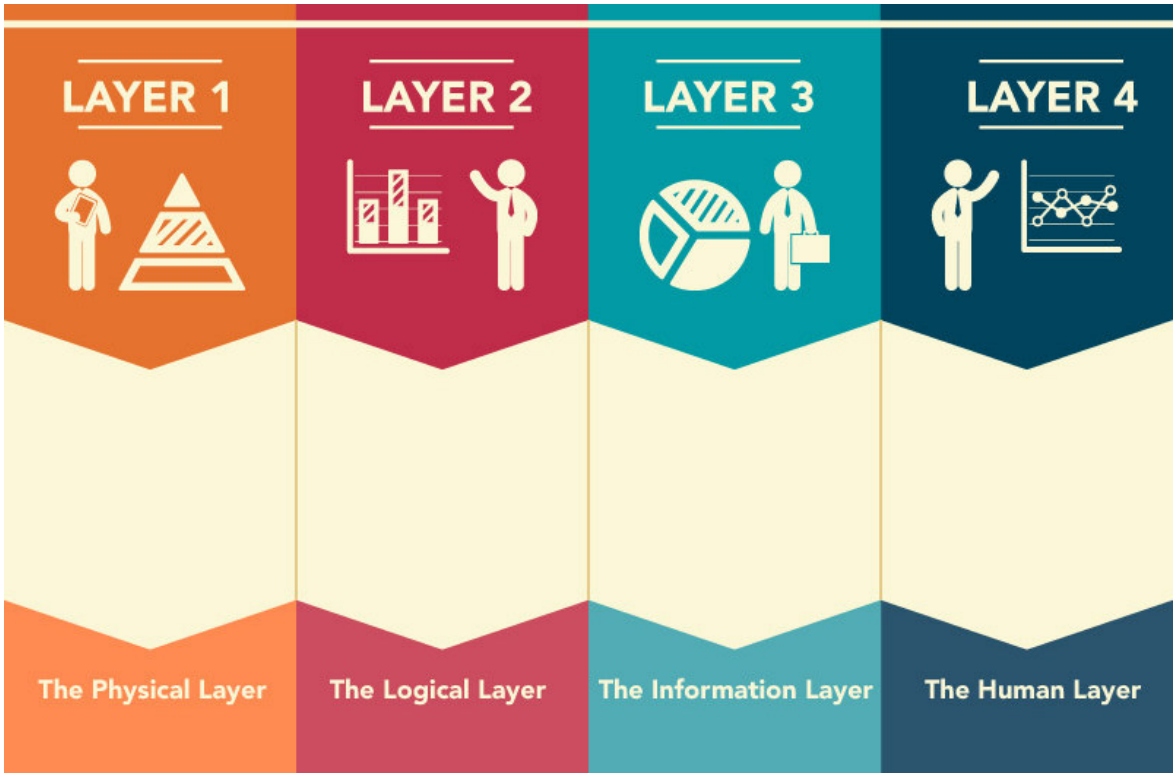


Fig. 2 Clark’s Cyberspace Model

The first layer, namely the physical layer of the cyberspace is the foundation of cyberspace—the physical devices out of which it is built. Cyberspace is a space of “interconnected computing devices, so its foundations are PCs and servers, supercomputers and grids, sensors and transducers, and the Internet and other sorts of networks and communications channels” (Clark, 2010, p.2). The communication occurs over these physical hardwares and it can be thought that the physical layer is perhaps the easiest part of the cyberspace to grasp (Clark, 2010, p.2), because

apparently it is tangible and its physicality gives it a sense of location, unlike other layers of the cyberspace. Physical devices such as routers or data centers do exist in a place and thus might be said to exist in a jurisdiction of a nation-state.

The second layer is the logical layer, and refers to the design, strengths and limitations of the cyberspace that are created or maintained by human logic (Clark, 2010, p.2). Clark defines this logical layer collectively as "the decisions that are made at the logical layer." For Clark (2010):

> it would have been possible to build a very different Internet within the constraints of the same physics. The decisions that shape the Internet arise at the higher layer—the logical layer where the platform nature of the Internet is defined and created. So that layer is going to be central to many of the considerations that arise when we analyze cyberspace, as will the layers that deal with information and with people. (p.2)

The logic of the cyberspace constitutes a layer of its own, since cyberspace, unlike the physical space or physical parts, has a logic which created it in the first place and maintains it the way it is, or in another way if deemed necessary.

The third layer that Clark defines is the information layer, which is easier to perceive for us. Clark defines the information layer of the cyberspace to be the whole information that is out there in the cyberspace such as webpages, media, texts, videos, or simply, knowledge. As it can be remembered from the cyberspace definitions that focus on its spaceness, it is this layer that gives the cyberspace a sense of being-in, a sense of physical space where one can have an existence in. Clark (2010) explains this information layer's content as follows:

> Information in cyberspace takes many forms—it is the music and videos we share, the stored records of businesses, and all of the pages in the World Wide Web. It is online books and photographs. It is information about information (meta-data). It is information created and retrieved as we search for other information (as is returned by Google). (p. 3)

As an important side note, Clark also states that the character of the information in cyberspace has been transformed greatly since the initial days of the Internet. The static information like static images or texts have been altered and they are now created more dynamically on demand, blurring the boundaries between storage and computation.

The fourth and last layer of the cyberspace, for Clark, is the human layer, namely the people who use all other layers of the cyberspace. Clark (2010) states that:

> People are not just the passive users of cyberspace, they define and shape its character by the ways they choose to use it. The people and their character, which may vary from region to region, is an important part of the character of cyberspace. If people contribute to Wikipedia, then Wikipedia exists. If people tweet, then Twitter exists. [...] So we must recognize people as an important component of cyberspace, just as we must recognize wires and protocols. (p. 4)

As it can be seen from all the definitions other than that of Clark's, there is something that is missing from each of them. They mostly focus on either the cyberspace's being a network (which it physically is,) or the "spaceness," the information that is stored on somewhere on the other side of the network. However, Clark's definition combines all the possible components of cyberspace and organizes them under a neat scheme. Clark's model is therefore especially helpful for such a study, where physical information and human layers of cyberspace are all relevant and need to be taken into consideration.

## 2.4 A brief history of cyberspace

In order to truly understand the nature and thus the description of the cyberspace, the definitions alone do not suffice and it is necessary to have a brief look at the history of cyberspace and how it came to dominate human lives in the last

years to an unprecedented extent. The "astronomical expansion" that Kuehl emphasized in one of the quotes above regarding cyberspace can be visually understood from the two time graphs below. The realization of cyberspace as *the* technology of the twenty-first century was simultaneously matched with the drastically increased number of Internet hosts (that are used to reach to cyberspace,) and the number of websites that are registered (and stored) which can be conceived as the landing points thus the "territory" of the cyberspace.

The graph in Figure 3 shows the increase of Internet hosts since the year 1995, in exponentially growing numbers. The year 2004 witnessed another momentum, for various reasons.

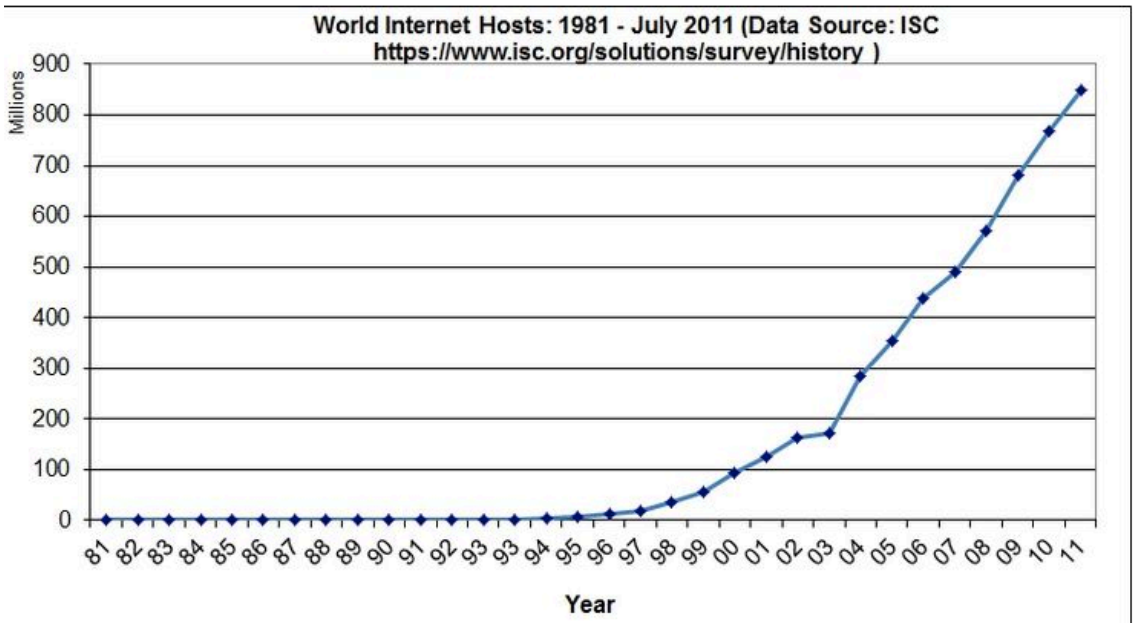

Fig. 3 World Internet Hosts, 1981 – July 2011 (Source: ISC, 2016)

The graph in Figure 4 visualizes the number of websites since the beginning of 1990s and clearly indicates the number of websites throughout the second half of the decade. Especially after the dawn of the millennium, the number increased in an astronomical fashion, and eventually reached a point today, where it is almost impossible to detect in nominal numbers. The number of websites can be

metaphorically thought to be the number of "acres" of the cyber "territory" which expands permanently and irreversibly.

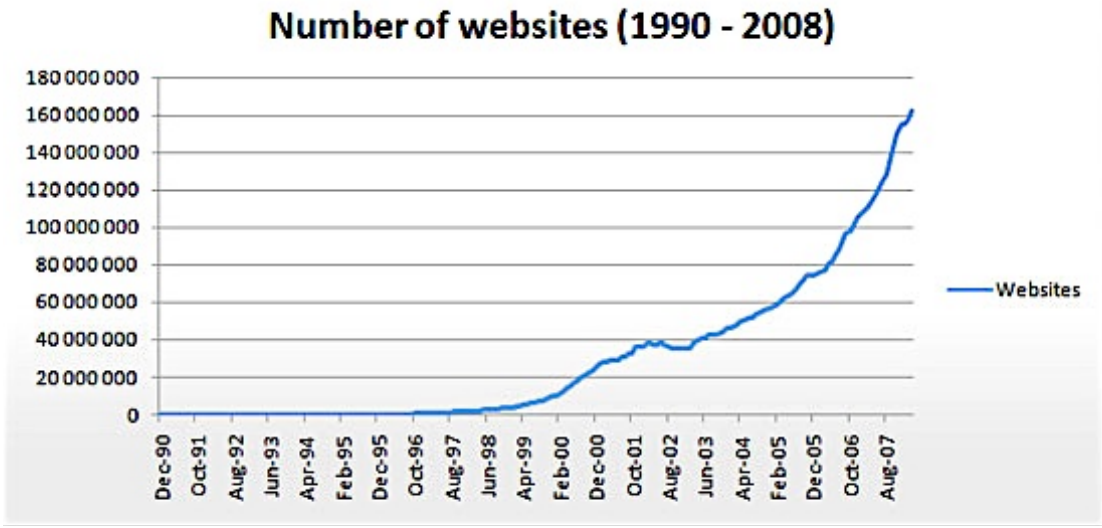


Fig. 4 Number of Websites (1990 – 2008) (Source: ISC, 2016)

One of the main characteristics of cyberspace that should be noted is that, unlike other technological and communicational advances, cyberspace constitutes a space where it is not under the direct control of any nation state or agent. It is true, however, that the US maintains some hegemonic power over the use and development of the cyberspace through various mechanisms. The Internet Corporation for Assigned Names and Numbers (ICANN), for instance, the institution that ascribes web domain names and addresses to the entire world, is judicially subject to Californian state law, which results in the opposition from many other nation states. BRICS countries, for instance, fiercely oppose this debated role of ICANN and the US cyber dominance (Ebert & Maurer, 2013). The US hegemonic power is not restricted to ICANN's role, since the US is also the country from which almost all of the developments regarding cyberspace stem. This sort of US dominance aside, however, it should be noted that the cyberspace is something that can be reached from anywhere in the world, given that the hardware required to

access it are available. This decentralized nature of cyberspace poses a quite interesting case, since, while the hardware are located within the nation state borders, the cyberspace is not. Cyberspace is thus, at least up to now, on its own. Internet is, arguably, literally "decentralized" (Post, 2009, p. 28). Most of the researchers emphasize this feature of cyberspace, as epitomized in Lessig's words:

> [S]omething fundamental has changed… Cyberspace presents something new for those who think about regulation and freedom. It demands a new understanding of how regulation works and of what regulates life there. It compels us to look beyond the traditional lawyer's scope – beyond laws, regulations, and norms… In cyberspace we must understand how code regulates – how the software and hardware that make cyberspace what it is regulate cyberspace as it is. As William Mitchell puts it, this code is cyberspace's "law." *Code is law.*" (Post, 2009)

The word cyberspace itself was actually coined by Gibson in his science fiction literary work. The novel is one of the examples of the cyber punk literature, which, unrelated to the Internet, started writing about a vision regarding a future where humans and electronic devices are merged. Although this was not ever achieved, the term itself caught the attention of the technicians and engineers in the novel. The significant passage from the novel where cyberspace was first used is as follows:

> The matrix has its roots in primitive arcade games,' said the voice-over, 'in early graphics programs and military experimentation with cranial jacks.' On the Sony, a two-dimensional space war faded behind a forest of mathematically generated ferns, demonstrating the spatial possibilities of logarithmic spirals; cold blue military footage burned through, lab animals wired into test systems, helmets feeding into fire control circuits of tanks and war planes. Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding... (Gibson, 1984, p. 67)

The later years, when the Internet took hold as a virtual space, which was most akin to the cyberspace term used in the novel, it was increasingly used to denote the Internet. “The term "Cyberspace" started to become a de facto synonym for the Internet, and later the World Wide Web, during the 1990s, especially in academic circle” (Vanderbilt University, 1996). The word cyberspace was first used to refer to the existing Internet network by John Perry Barlow. Barlow first used the term cyberspace to refer to "the present-day nexus of computer and telecommunications networks." Barlow (1990) describes it thus in his essay to announce the formation of the Electronic Frontier Foundation (note the spatial metaphor) in June:

> In this silent world, all conversation is typed. To enter it, one forsakes both body and place and becomes a thing of words alone. You can see what your neighbors are saying (or recently said), but not what either they or their physical surroundings look like. Town meetings are continuous and discussions rage on everything from sexual kinks to depreciation schedules. Whether by one telephonic tendril or millions, they are all connected to one another. Collectively, they form what their inhabitants call the Net. It extends across that immense region of electron states, microwaves, magnetic fields, light pulses and thought which sci-fi writer William Gibson named Cyberspace.

The use of the word cyberspace in the literary works aside, the history of the Internet we use today could be said to start with the first packet switching network, ARPANET. Although the concept of data communication over a network is really old, the first successful message on the ARPANET was sent from computer science Professor Leonard Kleinrock's laboratory at University of California, Los Angeles (UCLA) to the second network node at Stanford Research Institute (SRI). ARPANET, “a network composed of small computers called Interface Message Processors (or IMPs), similar to the later concept of routers, that functioned as gateways interconnecting local resources” (Living Internet, 2015). After the successful trial of communication between two centers, a 4-node network was connected by some other universities. The number of hosts grew to 213 by 1981

(Hafner, 1998) and ARPANET became the technical core of what would become the Internet, and a primary tool in developing the technologies used. In early 1983, ARPANET started using the TCP/IP protocol, a movement that can be considered as the start of the modern Internet (Postel, 1981). The TCP/IP protocol requires a rather long technical treatise to understand for a non-technical reader, so it is best to keep short its explanation here. TCP/IP provides end-to-end connectivity specifying how data should be packetized, addressed, transmitted, routed and received at the destination. The real logic of the TCP/IP is that, anything can be added to the network anywhere, anytime, endlessly. This is the main feature of this protocol and what makes the internet network "the Internet". David Post (2009) explains the simple yet powerful logic of TCP/IP network as "being able to add any of them to an existing network at any point on that network" (p. 89). He goes on as follows: "During the ensuing two decades, it was TCP/IP that triumphed, TCP/IP network that outgrew them all." And Post (2009) presents the reason why: "Why? It didn't grow so fast or become so big because it was "the Internet;" it became "the Internet" because it grew so fast and became so big" (p. 46).

In addition to the ARPANET network that is explained in the previous paragraph, there were a few other experimental networks in the United States, again used in the universities and other military circles. The US Military Research Agency accepted to fund the research and the unification of the smaller networks to the ARPANET was realized. Figure 5 visualizes this.

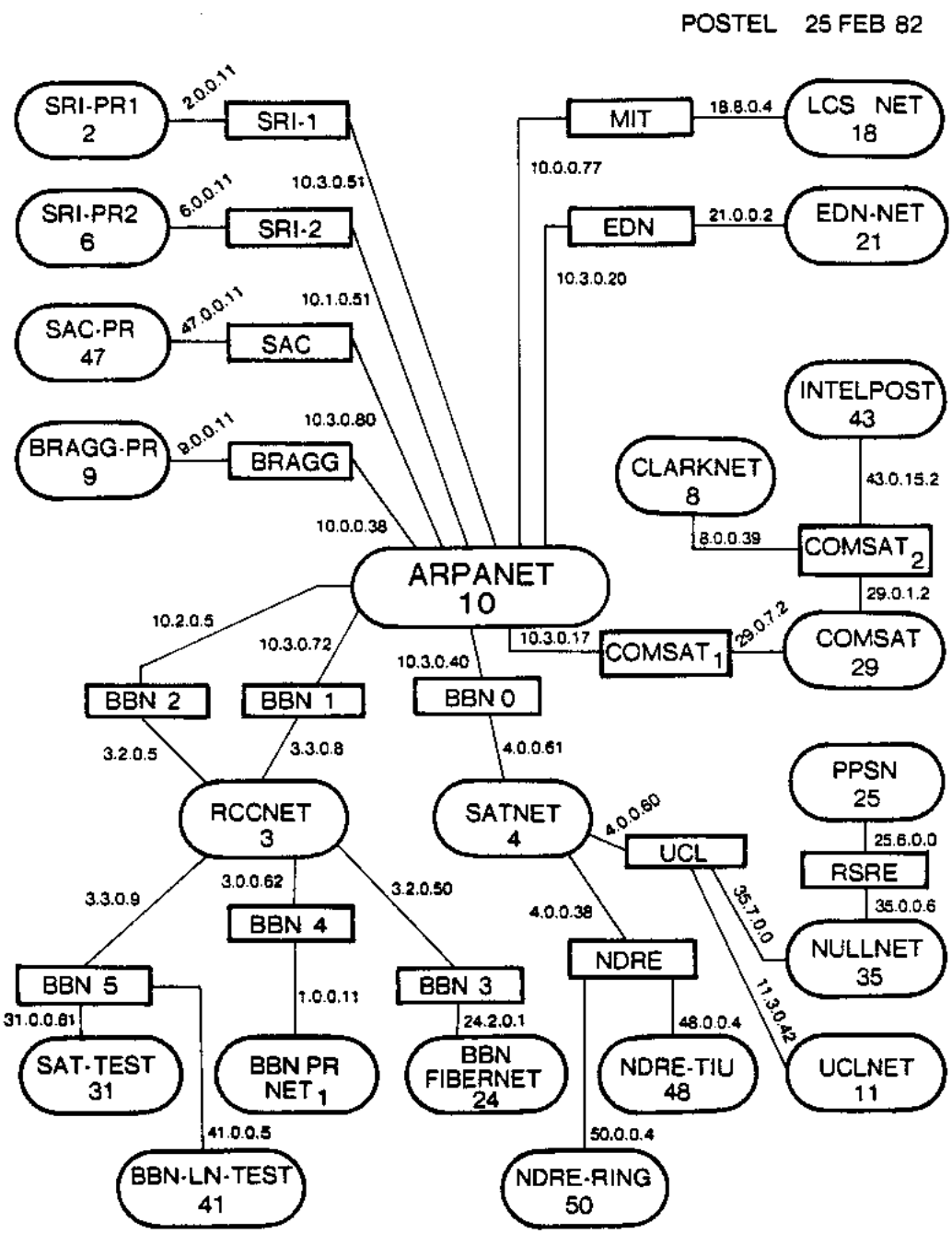


Fig.5 The TCP/IP network with the participation of smaller networks, February 1982 (Source: Arpanet Map by John Postel)

In the years between 1984 and 1988, the European research agency CERN also developed a network within itself using the TCP/IP network and it was connected to the American network through the end of the 1980s, alongside with some Australian

universities. In the late 1980s, the term “Internet” was adopted as an abbreviation of the term “internetworking” and the two terms started to be used interchangeably (Tanenbaum, 1996). Asian centers also connected to this US network in the 1980s, with Japan, Singapore and Thailand taking the lead. The “global divide” that divides the developed and developing countries in terms of their connectivity to the Internet which even persists today, started to be experienced in that period, since the developing countries needed to wait at least two decades to be able to fully connect to the Net.

As can be seen from the above information, initially, as with its predecessor networks, the system that would evolve into the Internet was primarily for university and government use. But in the 1990s, the Internet saw its use in the wider societies, as the Internet Service Providers (ISPs) started providing commercial Internet to the research centers and institutional users. The World Wide Web, which carries the logic that web sources are to be identified by URLs and be accessed via the Internet using a web browser, came into use. With the use of the emails and other web content, the Internet was introduced into larger public and 2010s were the years when social media use came into the picture, reaching billions of active Internet users. Internet governance, the question of how the Internet is going to be governed internationally is still a hotly debated topic. The fact that the Internet Corporation for Assigned Names and Numbers (ICANN) is located in the United States raises concerns internationally; especially from the states aspiring to be global powers themselves, such as Russia or France. ICANN is a nonprofit organization, organized from the Secretary of State of the State of California in the U.S. that is responsible for coordinating the maintenance and methodologies of several databases, with unique identifiers, related to the namespaces of the Internet - and thereby, ensuring

the network's stable and secure operation (ICANN, 2016). Just because of this overly significant role of the corporation, its role is constantly debated at every international occasion regarding the Internet governance.

As mentioned previously and pretty briefly, there exists a global gap between the countries in terms of their connectivity to the Internet. The developed-developing, or the famous North-South divide, is completely visible in the Internet connectivity maps produced for various purposes. One such map is presented in Figure 6, which quite clearly shows the immense gap between the Internet connectivity rates of the populations in the world, as a percentage of their country's population. While the Internet connectivity rate is well above 80% in the US and the Northern European countries, meaning that almost the whole population is active on the cyberspace, the rate drops to below 20% in the African or South Asian nations.

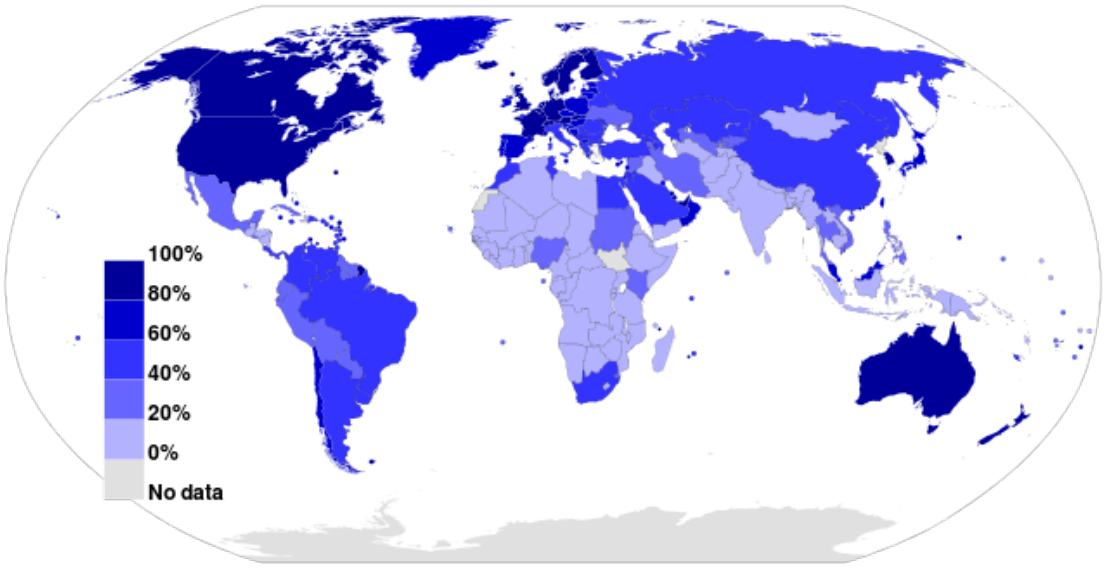


Fig. 6 Internet users in 2012 as a percentage of a country's population (Source: International Telecommunications Union, 2013)

In addition, Figure 7 shows an important fact about the content of the cyberspace in terms of their language statistics.

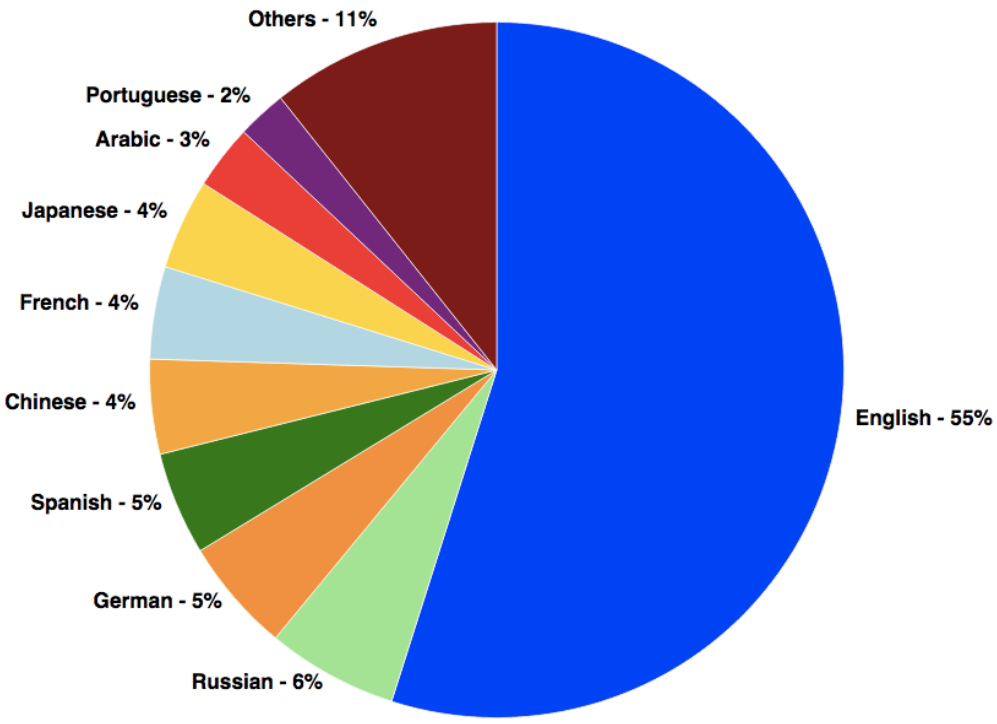


Fig. 7 Content languages for websites over the Internet (Source: w3tech.com)

The content of the cyberspace is overdominantly in English, while the languages that are spoken in the world such as Mandarin, Arabic or Portuguese have only marginal existences in the cyberspace, and the languages such as Bengali, Hindi or Urdu cannot even be seen in the language graphs.

After looking at the history of the cyberspace, it will be now suitable to look at how the cyberspace, throughout the period of its development, has been studied in the various disciplines of social sciences.

## 2.5 Cyberspace studies in social sciences

It is difficult to argue that the cyberspace has been extensively studied in the various disciplines of the social sciences and it is possible to feel some kind of abstinence from, or awkwardness towards, the cyberspace studies by the social scientists. Cyberspace is still an avoided subject, left mostly to technical scientists, for the reasons specified above. However few or incomprehensive they might be, the

cyberspace research in social sciences is taking hold and increasing in number. The fact that cyberspace has consolidated itself as one of the central domains of the modern human life since the beginning of the 1990s has been matched with a gradually heightened interest in social sciences towards it.

When all the literature in social science regarding the cyberspace is reviewed, it is obviously seen that the cyberspace was still seen as marginal and distant in social studies up until the Arab Spring (whether it was a spring or not is not within the scope of this thesis,) during which the significance and central role of the cyberspace was entirely realized. Since then, the increase in the cyberspace studies has been immense and the social scientists have tended towards mentioning cyberspace alongside with the street movements, protests, activism and all kinds of other mobilization. It is hard nowadays to find any study regarding social groups, terrorism, activism, mobilization or socialization that does not dedicate a chapter or a part to the use or abuse of cyberspace. If the cyberspace is now a factor that social scientists take into consideration, the questions that need to be answered are how various social sciences prefer to approach it and which analytical tools are employed in studying cyberspace.

The cyberspace is studied by many social sciences with the obvious exception of, perhaps, history. In sociology, psychology, and social psychology disciplines, for instance, cyberspace is studied for its potential to bring together social groups, to alter the mindset of any individual connecting to the cyberspace and to mobilize as a part of a cyber or non-cyber group. These disciplines focus mostly on how the cyber and real world differ in their social processes, psychological structures and such.

Alongside sociology and psychology, political economy also focuses on the cyberspace as an economic factor that also had political consequences. Whether the

cyberspace is a force that will foster the privatization and neo-liberalization in the economy of a country is a largely discussed topic. The proponents of the Marxist camp were mostly pessimistic since the cyberspace was at the hands of the private sector from its initial stages onwards; while the proponents stemming from the neoliberal camp showed more optimistic tendencies. This debate coincided with the beginning of the 1990s, which was the time of the dissolution of the socialist countries and neoliberal economic solutions tried in them.

In the 1990s, cyberspace was especially approached by some political scientists who studied it by the analytical tools of political science. Most of this literature, which is predominantly related to the relationship between sovereignty and cyberspace, is reviewed in Chapter 4 of this thesis. Other than these works, political scientists were also interested in the potential relationship between democracy and cyberspace. In line with the political context of the 1990s when the transitions to democracy and the dynamics that led to the successful – and failed – transitions to democracy were extensively studied, cyberspace was evaluated in the same vein, however primitive and undeveloped it was at the time. The primary reason that caused such mostly optimistic democratic expectations from the cyberspace was the belief that cyberspace constituted a virtual arena where everyone can be represented and can vote, express his/her thoughts and participate in the decision-making processes, just as the Athenian direct democracy. While the proponents of this optimism wrote such analyses, many other, especially Marxist-oriented political scientists saw no potential in cyberspace for further democracy, focusing on the apparent and inevitable fact that cyberspace, or rather, the means to access to, or exist in, the cyberspace, was already privatized and thus "not public," diminishing the prospects of cyberspace for democracy, if any.

The political science literature regarding cyberspace was almost stuck in the end of the 1990s and with the new millennium, cyberspace studies seem to have shifted to some other disciplines. The realization that the cyber power would be a significant part of political and military power, a phenomenon called "cyber security," emerged, and cyberspace-related analyses came to be handled in the disciplines like the International Relations, Security Studies and Military Studies. With the realization that the social and political life would be too dependent on cyberspace in close future and that cyberspace might be used to hack and affect the critical infrastructure of the countries, international relations scholars included cyber security into their conventional international relations works. For instance, how the novel cyber capabilities of countries can affect the relations among nations, how the use of cyberspace can be fitted into the existing international relations theories and which countries are more likely to affect, and be affected by, the new power equations are among the academic research areas of these scholars. Just to give a few outstanding examples, for instance, one of the scholars who understand the significance of cyberspace in international affairs, Joseph Nye, is of the opinion that "In the past, when an attack was intended, an aircraft or a tank needed to pass a border, but today, only electrons need to pass a border. When cyber is concerned, offensive moves are easier than the defensive moves, and it is getting increasingly difficult to counter the cyber attacks," which he argues over and over again in his works (Nye, 2014).

Just like the international relations discipline, cyber security concerns also jumped into security and military studies. As previously mentioned, the cyberspace as a factor in international power relations is the subject of cyberspace studies in international relations discipline; and in security studies, the analyzes about the

cyberspace are also similar. In addition to this kind of focus, the security studies are also concerned with the question of how cyber capabilities of a state can be incorporated into the conventional military structures. In other words, how a cyber unit (composed of "white-hat hackers") can take place in a military, to which corps such a cyber military unit can be attached (air corps, navy, or as a distinct unit itself?), how to benefit in sensitive institutions such as the military or intelligence organizations from the cyber experts who hold (mostly) illegally-oriented pasts are the sample questions the security and military studies approach cyberspace or cyber security.

Under security studies, the cyber terrorism research has also taken hold and has been increasing ever since the cyberspace was first used for terrorism purposes. Cyberspace, as it can be seen from the later chapters of this thesis, especially the Chapters 5 and 6, provides an ample ground for terrorist activities because of the inherent anonymity it provides and its power of reaching masses in extremely short amounts of time. Because of this reason, cyberspace use is extremely popular now in almost all terrorist activities, both in the planning processes of these activities and, in the aftermath of the terrorist acts, in order to create havoc and multiply the psychological impact of a successfully conducted terrorist act. Due to this reason, the terrorism researchers in the disciplines such as political science, international relations and security studies all recognized the potential of the cyberspace and they have included it in their studies, sometimes as an independent, and sometimes as a dependent variable. When we look at the studies or analyzes regarding ISIS, one of the most important terrorist organizations in the history of the world, for instance, we see that the use of cyberspace is a central tenet of this terrorist organization. ISIS uses cyberspace so effectively that it not only recruits thousands of fighters from

around the world every month through its social media accounts, but it also functions exactly like an effective nation-state (which it actually claims to be) in the cyberspace through its “ministries” or other “institutional” propaganda accounts.

In the most recent years, in addition to International Relations and security studies, Law and International Law are also increasingly concerned with the role of cyberspace in them. Law, for instance, tries to place cyberspace in human, economic or social relations amongst the individuals or companies, what the rights and responsibilities of them in cyberspace are and how they can be codified. It is difficult to find a country in the world now which does not incorporate cyberspace into its legal provisions and which has not defined cyber rights and cyber crimes. As Cyberspace Law and Policy Community’s webpage sums it up, legal provisions have been already drafted in many countries regarding a wide array of crimes such as information breaches, child pornography, digital signature related crimes, tampering with computer source code, hacking, malware production and cyber terrorism (Cyberspace Law and Policy Community, 2014).

In International Law, the cyberspace is one of the recent hot topics that is frequently made subject of studies in increasing numbers. This discipline is concerned with the question of what kind of a legal status cyberspace has, or will have, in international affairs and how the cases amongst the states regarding the use of cyberspace will be resolved. The most updated literature in international law views cyberspace as just like the conventional territory of a nation state, and tries to view the cyberspace cases that might arise in the future in the light of the previous international cases, tribunal decisions or arbitrations. NATO, in the recent years, is actively pursuing to be the leading research body regarding the cyberspace, through one of its many centers of excellence, the Cooperative Cyber Defense Center of

Excellence based in Tallinn, Estonia. The most significant study, among many publications that this center has published, is the Tallinn Manual, which applies the existing law of jus ad bellum to the cyberspace and cyber conflicts. The provisions of the warfare law in existence are hypothetically applied to the cyber conflicts in this Manual, which serves as a basic reference guide for future research and a basis for further international legal regulations regarding cyberspace. The document has not been signed or officially approved by any state yet, so it is just in the form of a text of sheer academic interest, however, the mere existence of such a study is extremely significant for the formation of further legal provisions in the future. The reception for the Tallinn Manual was so intense and positive that the same team of researchers gathered again to draft and publish the Tallinn Manual 2.0, which will further specify the legal role of the cyberspace, especially in the peacetime.

This chapter reviews the characteristics, definitions, history and models of the cyberspace as it takes place in a scattered array of places and disciplines. This kind of an introduction is necessary for the development of the arguments in the thesis. The chapter also reviews how the cyberspace has been handled in the social science disciplines such as sociology, psychology, international relations, political science, security studies, law and international law. It should be noted once again that the thesis is going to build its arguments on the cyberspace model by David Clark, leaving aside many other cyberspace definitions and models. The next chapter is on the concept of sovereignty, the dependent variable of the thesis, and it is thus one of the building blocks of the thesis. The cyberspace, according to the comprehensive definition provided by Clark, consists of four different layers, and by its being in the center of human life, has various definite implications for the nation-state

sovereignty. In order to scrutinize what implications the cyberspace might mean for sovereignty, it is necessary to have a look at the concept of sovereignty at length.

# CHAPTER 3

# THE CONCEPT SOVEREIGNTY

This chapter is devoted to explaining and analyzing the concept of sovereignty, which is required for the development of the thesis further in the subsequent chapters. Sovereignty is, actually, a word that is frequently used outside of the political science terminology. In the political science, however, it is used more than any other field, since it is one of the attributes of the nation states.

Sovereignty is one of the concepts that appear most frequently in both the political science literature and every other field directly or indirectly related to international relations. Though it is so often used and mentioned as one of the fundamental attributes of the nation states, the term does not have a clear-cut definition, which is agreed upon by the scholars. In Oppenheim & Roxburgh's (1920) words:

> There exists perhaps no conception the meaning of which is more controversial than that of sovereignty. It is an indisputable fact that this conception, from the moment when it was introduced into political science until the present day, has never had a meaning which was universally agreed upon. (p. 129)

Oppenheim, in the same political science work, goes on to find minimalist definitions for the term sovereignty and describes it simply as "the supreme authority, an authority which is independent of any other earthly authority" (Oppenheim & Roxburgh, 1920, p. 129). The term in this raw definition is further applied to the political science realm and "[s]overeignty in the strict and narrowest term implies, therefore, independence all round, within and without the borders of the country" (Oppenheim & Roxburgh, 1920, p. 129). The emphasis in this definition

aptly categorizes sovereignty into its two components, an inside and an outside sovereignty, which constitutes a dichotomic categorization that keeps recurring in almost all sovereignty analyses. The definitions of the term sovereignty throughout the twentieth century reflect more of less the same meaning as the one by Oppenheim. According to the *American Heritage Dictionary* sovereignty is "supremacy of authority or rule as exercised by a sovereign or sovereign state" or, alternatively, "complete independence and self-government."

A word already existing in theology and literature as referring to God, the concept of sovereignty had also been in use to refer to the kings and the similar political authorities over a certain territory or people. As a political attribute of the nation states, it underwent some transformations over the twentieth century (Henkin, 1999, p. 2). Sovereignty meant primarily political independence (Anghie, 1999; Taylor, 1997, pp. 757-58). Linked with this meaning, it also included the territorial integrity (UN Charter, 1945), and as a consequence, the jurisdiction and absolute control within a territory (UN Charter, 1945). These notions that are agreed to be included in the meaning of sovereignty are further confirmed and consolidated by the international legal cases, which all came up with a more or less similar definition of sovereignty. It can be realized from these definitions that they mostly represent a realist understanding of state and state sovereignty.

Sovereignty is also a key element in defining the state and the famous sociologist Max Weber's state definition holds a special place in the sovereignty definitions history. Max Weber's (1946) definition of the state is that "a state is a human community that (successfully) claims the monopoly of the legitimate use of physical force within a given territory." Weber's definition views the conditions of sovereignty as a legitimizing principle thus giving the state the authority to exist.

Building on Weber's definition, John Agnew views the relationship of state and sovereignty as essentially being about power. He explains "in conventional political discourse, sovereignty is about central state control and authority. […] From this viewpoint, state sovereignty may be understood as the absolute territorial organization of political authority" (Agnew, 1987).

Though sovereignty was surely thought to be the basic "given" tenet of the nation states, the written definitions of sovereignty are formulated mostly in the international law cases between clashing sovereignties of states in question. In one of the international law cases, which involved a violation of state sovereignty, Max Huber, as Arbitrator in the 1926 *Island of Palmas* case, wrote that "Sovereignty in the relations between states signifies independence. Independence in regard to a portion of the globe is the right to exercise there, to the exclusion of any other states, the function of a state" (Island of Palmas Case, 1926). As it can be seen from the decision, this definition also reflects the two-faced understanding of sovereignty, firstly "the right to exercise power on a territory" and secondly, "excluding the intervening of any other authority." The arbitrage decision also went into the details of sovereignty further, which sets a precedent for territorial sovereignty in international law up to date:

> [1] if there is a dispute over a territory, then the question of which of the competing sovereignties is stronger is important; [2] where a State challenges the sovereignty of another over a territory, the challenger must demonstrate that, in addition to establishing its sovereignty at a particular time, it has continued to exercise its sovereignty over the disputed territory.

The incident which resulted in the codification the meaning of the term sovereignty in international law properly, however, is yet another international law case, which was processed by the International Court of Justice. In the Arantzazu

Mendi case, the Court defined "sovereignty" as "a government which exercises *de facto* administrative control over a country and is not subordinate to any other government in that country or a foreign sovereign state" (House of Lords Decision, 1939). In this way, the House of Lords decided that the Nationalist Spanish government was "sovereign" over a specific territory and thus immune from local British courts since it was recognized by the UK (Abass, 2001, p. 145). In one of the other cases decided by the International Court of Justice, Judge Alvarez, in his individual opinion in the *Corfu Channel* case, wrote that, "By sovereignty, we understand that the whole body of rights and attributes which a state possesses in its territory, to the exclusion of other states, and also in its relations with other states" (International Court of Justice, 1949). Helmut Steinberger (1981), in the *Encyclopedia of Public International Law* puts forward that "Sovereignty… denotes that the basic international legal status of a state that is not subject, within its territorial jurisdiction, to the governmental, executive, legislative, or territorial jurisdiction of a foreign state or to foreign law other than public international law." (p. 408)

Louis Henkin, who is an ardent opponent of the term sovereignty, who goes so far as to call it the "S" word to avoid using the word "sovereignty" writes that this basic principle of international law and international relations as well as political science holds that "… except as limited by international law or treaty, each state is master of its own territory." In a lecture he gave at Fordham University School of Law, Henkin (1999) argued that "Its birth is illegitimate, and it has not aged well. The meaning of "sovereignty" is confused and its uses are various, some of them unworthy, some even destructive of human values." Throughout the lecture he

analyzed the transformations that caused the term to alter, and arrived at the conclusion that:

> And so, state sovereignty at the end of the end of the twentieth century – and at the beginning of the twenty-first – can be summarized as: "Sovereignty means 'leave us alone.' Sovereignty is: "We will engage in a minimal amount of cooperation, if we as sovereign states consent." Sovereignty is subject to some 'creeping' international human rights, to the extent that sovereign nations consent. In general, I fear sovereignty as we have known it is alive and well. (Henkin, 1999, p. 5)

Henkin expresses a rather negative understanding of the term sovereignty, since he approaches the topic from the human rights aspect, arguing that the concept sovereignty involves some human rights violations. It is noteworthy to note here that Henkin (1999) devotes a few sentences to cyberspace (after the international market), and its fuzzy and ambiguous relationship to sovereignty:

> The 'international market' is a related concept. We read and hear about 'the Market.' Where is the Market? Where is it physically or geographically? Under whose laws and under whose control? Who is sovereign in regard to the Market, or perhaps is the Market sovereign? […] Cyberspace – Where is cyberspace? Is it subject to state sovereignty? To the same state sovereignty? Is cyberspace sovereign? (p. 6)

The definitions discussed so far handle the concept sovereignty as a totality, though they almost all break it into its two dimensions, one external and one internal. The neorealist camp also made its contribution to the sovereignty literature and the first deeply analytical work, albeit a short one, was the article by the famous political scientist Stephen D. Krasner, in which he deconstructed the concept into four different (but interrelated) components of the term the nation states largely enjoy. The article titled *Abiding Sovereignty* (Krasner, 2001), as its name suggests, discusses the neorealist position that the nation state sovereignty is still prevalent in the current age, despite the claims that it is no longer a powerful attribute of the states. The primary importance and explanatory power of his article stems from the

fact that Krasner decomposed 'sovereignty' into its aspects, rather than using it as a monolithic term as the previous studies before him did, in keeping with his neorealist tendencies. In such a way, the studies that base themselves on Krasner's sovereignty types are analytically profound and convincing.

The first sovereignty type Krasner (2001) classifies is the "interdependence sovereignty." By this Krasner denotes "the ability of states to control movement across their borders" (p. 231). He adds that globalization and the international market eroded this type of sovereignty since states cannot regulate monetary issues within their border at their absolute free will due to capital flows in and out, together with the technological advances.

The second type of sovereignty for Krasner (2001) is the "domestic sovereignty" and it means "the authority structures within states and the ability of these structures to effectively regulate behavior." This means the inner state sovereignty and it directly involves the territorial aspect of the sovereignty that other analysts generally refer to as the inner sovereignty. It must be noted here that this type of sovereignty includes the power to control the acceptance or recognition of the authority as "the authority" for the subjects. This domestic sovereignty concept is fundamentally relevant for an effective analysis of a relationship of sovereignty and cyberspace (p. 231).

The 'Westphalian/Vettalian sovereignty' is what Krasner (2001) classifies as the third type of sovereignty, and it directly means the "exclusion of external sources of authority" (p. 232). Krasner adds that this exclusion principle translates into the non-intervention principle in the international law and international relations. The reason he calls this type of sovereignty aptly as 'Westphalian' is that in the Peace of Westphalia, the authorities asserted their sovereignties by excluding any other

authority in their territories some four hundred years ago, a milestone that set precedent for the international relations up to day.

The 'domestic sovereignty' that Krasner classifies falls generally within the realm of political science while the 'interdependence sovereignty' and 'Westphalian/Vettalian sovereignty' is related more to the international relations and international law, since they denote how nations behave vis-à-vis each other, what they are and what they are not according to each other. It means the most basic and renowned principle of the modern nation states which is the capability to keep other countries from intervening in your affairs in your territory, and the ability to maintain this capability effectively. Therefore, the sovereignty as used in the international affairs literature mostly refers to the Westphalian/Vettalian sovereignty according to Krasner's classification.

The fourth and last type of sovereignty for Krasner is the 'international legal sovereignty' according to Krasner (2001) and means the process and principle of recognizing states as states. This means the recognition of a state as a free and equal entity of the international order (p. 233).

The most significant feature of Krasner's classification is that it does not offer a monolithic sovereignty description and rather allows the analyses based on these sovereignty types to be analytically more profound and explanatory. For instance, for Krasner (2001), while Westphalian sovereignty of a state may be quite powerful and effective, the domestic sovereignty of that same state may be quite weak. This means that while the state can effectively exclude any intervening by other authorities and can jealously protect its free will, it may lack necessary apparatuses to control and monitor the activities going on within its borders, due to an array of different possible reasons. In such a way, in a study like this present one, it is possible to

detect which aspects of sovereignty are likely to erode and which ones can be expected to get stronger due to some reasons or for some time, although this thesis, rather than Krasner's sovereignty model, uses yet another, more simplistic sovereignty definition and model.

Though not detailed as Krasner's, Joel Trachtman comes up with a similar distinction between the components of the term sovereignty. In an article where he focused on cyberspace, sovereignty and jurisdiction, he distinguishes sovereignty into two, according to its scope. For Trachtman (1998), the first sovereignty type is called "conclusory sovereignty" and it means an understanding of sovereignty which includes and thus "concludes" everything (p. 563). It means unconstrained state power and denotes that sovereignty is an absolute state power on everything, inside and in the face of other sovereigns. Trachtman harshly criticizes this understanding of sovereignty, and argues that it is nothing more than an illusion and should only be thought as an ideal type. The second type of sovereignty definition for Trachtman (1998) is the "contingent sovereignty" and rather than including everything inside it, this type of sovereignty means "the powers we decide to assign to the state" (p. 564). In such a way, Trachtman still benefits from the explanatory power of the term sovereignty (which is still relevant in political studies) and at the same time gets rid of the attributes not necessarily included in the term. Trachtman, in one of his other works, uses yet another distinction criterion between two sovereignty types. This classification strongly resembles other sovereignty definitions and replicated in Krasner, as well. The "vertical sovereignty" for Trachtman (1994) means the vertical relationship of a state with its subjects and its ability to control them and their activities inside the territorial borders (p. 568). On the other hand the "horizontal

sovereignty" denotes the sovereignty of a state in the face of other states and non-state actors (Trachtman, 1994, p. 568).

These sovereignty definitions, each focusing on some different aspect of the term are actually more or less the same, as can be seen from the above review. They basically view sovereignty as a dyadic term, with an internal and external determinant. Internally, it stands for the degree of effectively controlling the activities and persons within the territory, whether real or legal. Externally, it means the protection of the territory in question from any other authority. As most of the definitions mostly entail, the concept is mostly a euphemism for state power, its capability to do what it wishes, but the sovereignty, in addition to this vector power, somehow includes the orientation of the power, such that, when the political scientists use the word, it usually denotes the target of the state power, be it external or internal. By sovereignty, therefore, something relational is meant, and the target vis-à-vis the nation state, is hinted in the meaning. The reason why a distinct chapter was opened for discussing the concept of sovereignty definitions and come up with the one that best fits the purposes of the current thesis, one that will serve both conveniently and theoretically the backbone of the cases that will follow. Though the concept is debated for various pages, it is apparent that the sovereignty concept is a vague one and needs a clear operationalization. In order for them to be used in this present thesis more effectively and clearly, we need an operationalization index to see the tenets of sovereignty, because simply stating that sovereignty is state power is not convincing and academically not sound.

The operationalization for the concept of sovereignty that this thesis needs comes from an essential work that was written to fill the gap in the sovereignty literature by three political science scholars. Ghani, Lockhart and Carnahan, very

rightly, start their sovereignty index work, the attributes that a sovereign state must have, with the following introduction:

> Legal recognition alone, however, does not suffice to define the sovereignty of a state. Many governments that are legally recognized as sovereign consistently fail to meet the basic prerequisites of a sovereign government. There is a clear gap between the de jure sovereignty that is assumed when, for example, international treaties are signed between "sovereign" states, and the de facto absent or compromised sovereignty that exists in many of these states. (p. 4)

As can be seen from the excerpt, the writers focus on a point that they see as a gap in the literature. Claiming alone that a state is sovereign does not mean anything and it remains still as a vague and elusive concept, far from being within the scope of studying academically. The authors, namely, Ghani, Lockhart and Carnahan (2005) thus draft their work which "delineates a framework which proposes a set of core functions that a sovereign state must perform in the modern world" (p. 5). This index, for them, is "a framework for the calculation of a sovereignty index through which the sovereignty of a state can be measured in a tractable fashion." They assert that the framework might be said to consist of ten functions of a state and "[o]nce this more quantitative framework is in place, the progress of or decline in state capabilities to perform each function severally as well as collectively can be assessed" (Ghani, Lockhart & Carnahan, 2005, p. 5).

For Ghani, Lockhart & Carnahan, the ten functions of a state are shown in Table 1.

Table 1. The Ten Functions of a Sovereign State

| |
|---|
| Legitimate monopoly on the means of violence |
| Administrative control |
| Management of public finances |
| Investment in human capital |
| Delineation of citizenship rights and duties |
| Provision of infrastructure services |
| Formation of the market |
| Management of the state's assets (including the environment, natural resources, and cultural assets) |
| International relations (including entering into international contracts and public barrowing) |
| Rule of law |

The first and foremost tenet of sovereignty for Ghani, Lockhard and Carnahan is "a legitimate monopoly on the means of violence" and as the chapter previously indicated, this is a famous definition by Max Weber. The authors take Weber's definition as the first indicator of sovereignty and they take it as a more "psychological" monopoly as "the legitimacy of the state's monopoly on violence as perceived by the citizens of the state that is the key to using this monopoly as a criterion of statehood. If the polity rejects the legitimacy of the state's monopoly on violence, then that monopoly is inherently unstable." For the authors, this can be maintained "by the presence or creation of credible institutions that provide checks and balances on the use of force; that the state itself must be constituted through, and accountable under, the rule of law" (Ghani, Lockhart & Carnahan, 2005, p. 6). The authors also assert that in order to measure the degree of state control of the means of violence within state borders, "both the extent to which the state can protect persons and property and the legitimacy of this protection must be assessed."

For the authors, the second indicator of sovereignty is "administrative control, as defined by both the breadth and depth of the reach of a state's authority over its territory." The authors also state the necessary requirements for securing

administrative control in a territory as "the existence of a coherent set of rules that determine the division of responsibilities horizontally and vertically across functions of the state and between hierarchical levels; the recruitment of civil servants; the spatial and functional division of administrative roles; and flows of resources." The administration structure of a state might vary from highly decentralized to highly federated depending on the historical and cultural context.

Besides these more "historical-sounding" sovereignty indicators, the authors add yet another sovereignty indicator which might sound like a tenet of especially contemporary states, namely, the public finances. For the authors, "[s]ound management of public finances in today's interdependent world is probably the most critical indicator of the autonomy of a state. No state can be sovereign while it relies on an external source to fund its ongoing operations" (Ghani, Lockhart & Carnahan, 2005, p. 7). The domestic revenue of a state and its dependence of foreign assistance are, as the authors claim, clear indicators of a state's sovereignty and whether it is increasing or decreasing over time. Included in this "public finance management" is the control over the actual number of taxpayers, industries and resources.

The fourth indicator in the operationalization of sovereignty by the aforementioned authors is the investments in human capital since, "without this investment, different groups become disenfranchised, which undermines the capacity of the economy to develop in the longer term, and therefore of the state to fund itself in the future" (Ghani, Lockhart & Carnahan, 2005, p. 7). A state's investments in human capital give lead to the capability of citizens as actors in the economy, polity and society, as the authors claim.

Yet another citizen-related indicator of sovereignty that authors define as the fifth indicator is "the delineation of citizenship rights and duties that cut across gender, ethnicity, race, class, spatial location and religion are critical to stability and prosperity" (Ghani, Lockhart & Carnahan, 2005, p. 8). How the state defines its citizens, how the citizens are related to the state in question, with what ties they are connected to the state mechanism are all bundled in this indicator, and they constitute one of the indicators of a state's sovereignty.

The sixth indicator of the sovereignty of a nation-state is, for the authors, is the provision of infrastructure services and a state might be said to be sovereign if it exerts full control over this. The creation, operation and maintenance of infrastructure, especially in the modern political context, are critical for the sovereignty of a state. A state's ability to provide transportation, water and energy, maintenance of security and administrative control, investment in human capital are all meant in this "provision of infrastructure" article asserted by the authors.

Formation of the market is considered to be the seventh indicator of the state sovereignty according to the sovereignty operationalization scheme of the authors. "[T]he formation and expansion of the legal market […] emerged as one of the most important functions of the state" (Ghani, Lockhart & Carnahan, 2005, p. 8) and this ability of state "depends on the establishment and protection of property rights including the provision of enforceable contract, corporate, insurance, bankruptcy, land, employment and environmental laws" (p. 8).

Building on the idea that a state's sovereignty is comprised, to a great extent, of the economic sovereignty, the authors put forward, as the eighth indicator of sovereignty, "the management of the state's assets (including the environment, natural resources, and cultural assets)" (Ghani, Lockhart & Carnahan, 2005, p. 8). As

the authors claim, “how the state handles the licensing of particular industries will determine whether wealth is created or destroyed through the licensing process, and also gives a clear indication of the nature of the operation of the state both to the domestic polity and the international observer” (Ghani, Lockhart & Carnahan, 2005, p. 8).

The ninth indicator of a state’s sovereignty level is “international relations (including entering into international contracts and public barrowing)” according to the authors. This is actually an indicator that has been mentioned as “horizontal sovereignty” or “external sovereignty” by some of the scholars that this chapter previously reviewed. The authors explain this article as follows: “The state’s authority over international relations encompasses the management of relations with other states, international bodies and private entities, and the authority and opportunity to enter into treaties and obligations with them” (Ghani, Lockhart & Carnahan, 2005, p. 8).

The tenth and last indicator put forward by the authors is the rule of law. “The rule of law is the most critical indicator as to whether the formal and informal rules of the game are aligned” (Ghani, Lockhart & Carnahan, 2005, p. 9) is the critical sentence used by the authors to highlight the importance of it in terms of the sovereignty of a state. The authors, however, do not really delve into the normative plain of this article and what is considered by a state as the rule of law can be different from a state to another one. It can, however, be accepted that a state’s ability in asserting and maintaining “a rule of law that is accepted as a rule of law by itself” is the indicator that the authors mean. Included in this are a stable policy environment, constitution of the state, succession of rulers on the basis of rules and

the persistence of policies from one government to another (Ghani, Lockhart & Carnahan, 2005, p. 9).

These are basically the indicators of the sovereignty level of a state put forward by Ghani, Lockhart & Carnahan as the operationalization of the fuzzy concept of sovereignty. The present thesis will adopt this operationalization as the basis of its sovereignty measurement throughout the cases that will support the main argument of the thesis. After looking at the "sovereignty" aspect of the thesis and the operationalization scheme that is adopted to refer to the sovereignty of nation states in the future chapters, now it is the correct time to move on to the chapter that reviews the literature of the sovereignty and cyberspace relationship.

# CHAPTER 4

# THE RELATIONSHIP BETWEEN CYBERSPACE AND SOVEREIGNTY

> "You can be merry with the king, you can share a joke with him. But as Thomas More used to say, it's like sporting with a tamed lion. You tousle its mane and pull its ears, but all the time you are thinking, those claws, those claws, those claws."
> Hillary Mantel – *Bring Up the Bodies*

As briefly and previously summarized under the subtitle regarding the cyberspace, the relationship between the cyberspace and nation-state sovereignty has been analyzed in the political science literature starting from the 1990s onwards. This chapter reviews this literature and lays down the primary points, strengths and weaknesses of the sovereignty-cyberspace analyses written by social scientists coming from various disciplines, mainly the political science and the international relations disciplines. All this literature on cyberspace-sovereignty issues is basically divided into two distinct groups in the chapter, for the reasons of academic convenience. It is sure that each work analyzes a different angle of the cyberspace and sovereignty relationship, which others might ignore, each work should therefore be considered unique in itself. However, within the scope of such a thesis, it would be both convenient and reader-friendly to pack them all into two basic camps.

The first group consists of the scholars' works which argue that the cyberspace is, or would be, a factor that undermines and erodes the classical nation-state sovereignty through various mechanisms. Some entries in this category focus on a different side of the story. While some of the works argue that cyberspace would erode state sovereignty since cyberspace could turn into a platform where non-state actors exert themselves on, some other works in this camp still have the same claim, but based on the fact that cyberspace is developed and maintained mostly by the

private sector. Though their focus points differ, the works in this first group can all be said to argue that cyberspace has the potential to erode state sovereignty.

The second group, on the other hand, consists of the research pieces that view cyberspace as having an ample ground for strengthening state sovereignty. The general underlying reason for this is the fact that state is one of the stakeholders of the cyberspace since the initial stages of its development. The other significant basis of this line of thinking is the countless methods the states have been increasingly using within the cyberspace, such as filtering or censorship tools, hackings or simply the state dominance in the physical infrastructure of the cyberspace. For these reasons, the researchers categorized under the second group can be said to argue that the cyberspace strengthens the state sovereignty, in general.

As the Internet started to grow in the second half of the 1980s, political scientists realized the political potential of the cyberspace, however premature it might then be, and started asking analytical questions like whether this novel domain would hold any significant meaning for the political and social aspects of human lives. However, due to some obvious reasons, the cyberspace studies back then revolved around some vicious circles and ideological stances. The first and foremost reason for this is the fact that cyberspace was still in the making and was far from being consolidated as a domain where both public and private sectors, together with the individuals themselves, led an existence, as it is now.

Secondly, as illustrated previously by the graphs in the cyberspace chapter, the access to cyberspace was limited to a few specific official institutions and organizations and thus it was not quite possible to speak of a one-and-for-all sort of domain back then, as it is now again.

Thirdly, and most interestingly, the cyberspace analyzes in the time strictly reflected the political and economic context of the decade, which coincided with the dissolution of the Soviet Union and the following democratization and neo-liberalization policies in the Eastern European countries. Most of the political analyzes about the fledgling cyberspace were thus economics-related and they restricted themselves to a debate whether cyberspace will be dominated by state (state meaning mostly the public, in keeping with the leftist-oriented paradigm,) or the private sector (which is thought to be "the opponent" of the public, in keeping with the leftist paradigm, as well.)

## 4.1 Context of the cyberspace-sovereignty literature

The spirit of the beginning of the 1990s, which corresponded with the evolution of cyberspace, clearly reflected a rupture from the past, or rather, the final perfection point of history, and the beginning of a wholly new political and social structure. The epitome of this spirit is the book by Francis Fukuyama, published in 1992, titled as *The End of History and the Last Man*. The book mainly argues that, with the collapse of the socialist economic and political models that the world had just witnessed, the Western liberal democracy and capitalism were shown to be superior and better than any others, signaling the final endpoint of humanity's sociocultural evolution and the final form of human government. Arguing the total opposite of the Marxist predictions of final form of a system, Fukuyama (1992) stated that:

> What we may be witnessing is not just the end of the Cold War, or the passing of a particular period of postwar history, but the end of history as such: that is, the endpoint of mankind's ideological evolution and the universalization of Western liberal democracy as the final form of human government.

This kind of thinking, put forward boldly by Fukuyama, dominated the scene of the political science literature generally. In addition to Fukuyama, a heightened interest in a "new world" was also clearly reflected in an extremely famous article by Anne-Marie Slaughter. Although they were not specifically related to the cyberspace, the academic position advocating that the technological changes and advances will bring about an entirely new political order and social landscape together with revolutionary changes to the extant one had a few examples scattered around the minor and major news and political platforms around the decade and one of the most influential one was the article by Anne-Marie Slaughter published on *Foreign Affairs* in 1997, around the time when cyberspace-sovereignty debate was triggered. Slaughter, in her article, basically argues that a new world order is on the way and she analyzes the dynamics of this new world order. Slaughter (1997) puts forward that:

> A new world order is emerging, with less fanfare but more substance than either the liberal internationalist or new medievalist visions. The state is not disappearing, it is disaggregating into its separate, functionally distinct parts. These parts – courts, regulatory agencies, executives, and even legislatures – are networking with their counterparts abroad, creating a dense web of relations that constitutes a new, transgovernmental order. (p.183)

The ideas in Slaughter's article were inspired by an article of Jessica Matthews, published in 1997 on *Foreign Affairs* and reviewed below. The context in which cyberspace analyses took hold also witnessed a parallel literature, that of the globalization. The globalization phenomenon, which included the capital flows, the incredible amount and speed of transnational transactions of capital and labor, the cultural dominance of the West in the whole world, and the technological advances bringing the world together was rampant and quite fashionable to talk about at the time. For instance, the influential study by Frances Cairncross, *The Death of*

*Distance*, argues that new communications technologies are rapidly obliterating distance as a relevant factor in how we conduct our business and personal lives. About the irrelevance of the distance in the twenty first century, Cairncross puts forward that, "It offers a peek at the communications future: a world in which transmitting information costs almost nothing, in which distance is irrelevant, and in which any amount of content is instantly accessible – but only a peek, for the Internet is merely a prototype for something more sophisticated" (Cairncross, 2001, p. 76).

The context in which the literature of cyberspace and sovereignty started off was like this and the relevant literature had surely imprints of the period. The group of scholars that advocate that the cyberspace would ultimately erode the state sovereignty is reviewed firstly, since they are less in number.

## 4.2 Studies arguing the erosion of sovereignty by cyberspace

"We reject: kings, presidents and voting.
We believe in: rough consensus and running code."
David Clarke, the founder of the Internet

"Governments of the industrial world, you weary giants of flesh and steel,
I come from cyberspace, the new income of Mind. On behalf of the future,
I ask you of the past to leave us alone. You are not welcome among us. You
have no sovereignty where we gather."
(Barlow, 1996)

In the 1990s, the spirit of "change" and the aura of a "new world" were celebrated, so to speak, in the academic literature through other works as well, each social scientist trying to frame and explain this change, and the political science was an ardent area in which political scientists tried to come up with the dynamics, formations, reasons and results of this proclaimed "change." As the end of the 1990s drew near, with the millennium, the visible end of a thousand years, at sight, a handful of massively influential works in this fashion got published the most

significant (and the most relevant for this thesis) of which is the article by Jessica Matthews, published in 1997 on *Foreign Affairs*. Chosen by the journal's editors as "one of the most influential in the journal's 75 years" (Naidoo, 2000), the article boldly and straightforwardly announces that the national governments, or nation states, are losing their power vis-à-vis other actors, and it describes a shift away from the state – up, down, and sideways – to supra-state, sub-state, and, above all, to non-state actors (Mathews, 1997). The punch line, the most significant point of the article, is that it attributes this transformation to the "information technology," which she regards as the engine of the transformation:

> The most powerful engine of change in the relative decline of states and the rise of nonstate actors is the computer and telecommunications revolution, whose deep political and social consequences have been almost completely ignored. Widely accessible and affordable technology has broken governments' monopoly on the collection and management of large amounts of information and deprived governments of the deference they enjoyed because of it. In every sphere of activity, instantaneous access to information and the ability to put it to use multiplies the number of players who matter and reduces the number who command great authority. The effect on the loudest voice which has been government's has been the greatest. (Mathews, 1997)

It is true that Mathews does not specifically name the cyberspace in her study, but it is clear from the quotes that what she means by the information technology refers mostly to the cyberspace. Her exact wording deserves to be directly quoted, since hers is the most fundamental basic study regarding the erosion of state sovereignty and state power by means of the cyberspace, "the information technology" in her words. She refers to the cyberspace also as a "network" and goes on to the decentralized nature of it, almost surprisingly, given her limited technical knowledge and predictions:

> Above all, the information technologies disrupt hierarchies, spreading power among more people and groups. In drastically lowering the costs of communication, consultation, and coordination, they favor decentralized networks over other modes of organization. In a network, individuals or groups link for joint action without building a physical or formal institutional presence. Networks have no person at the top and no center. Instead, they have multiple nodes where collections of individuals or groups interact for different purposes. Businesses, citizens organizations, ethnic groups, and crime cartels have all readily adopted the network model. Governments, on the other hand, are quintessential hierarchies, wedded to an organizational form incompatible with all that the new technologies make possible. (Mathews, 1997)

It must be noted that Mathews' points and her way of handling the topic are wondrous, firstly because they are the first steps regarding the realization of the significance of the information technology for political science, and secondly because she realized the decentralized nature of the cyberspace, though cyberspace was not even so developed at the time. However, when we retrospectively look at Mathews' article, it can be seen that she ignored the massive potential of cyberspace to be used by the nation states themselves. Mathews can be excused for not predicting the use of information technology by the sovereign states, since the state practices such as filtering, censorship and monitoring techniques were not known at the time the article was written. Her points, regardless of the counter-arguments that might refute them at times, are important to note. The strengthening potential of the cyberspace for the non-state factors, she emphasizes again and again:

> The evolution of information and communications technology, which has only just begun, will probably heavily favor non-state entities, including those not yet envisaged, over states. The new technologies encourage non-institutional, shifting networks over the fixed bureaucratic hierarchies that are the hallmark of the single-voiced sovereign state. They dissolve issues' and institutions' ties to a fixed place. And by greatly empowering individuals, they weaken the relative attachment to community, of which the preeminent one in modern society is the nation state. (Mathews, 1997)

In addition to this article of Mathews, the academic debate that explored the implications of cyberspace in terms of sovereignty, and political science in general, started off with a rather influential and classical article by Henry H. Perritt, Jr., which is reviewed in this chapter under the studies that claim the strengthening of sovereignty under cyberspace. Perritt (1998) quite self-explanatorily named his article "The Internet as a Threat to Sovereignty?" where he discussed his arguments regarding whether the Internet, though in very initial stages at the time, is a factor that will undermine or strengthen state sovereignty. The triggering inspiration that underlies Perritt's writing his analysis is an article by Wriston, just like that of Mathews', where Wriston basically and quite prematurely argues that "[s]overeignty, the power of a nation to stop others from interfering in its internal affairs, is rapidly eroding" (Wriston, 1997, p. 174). The article cites, in addition to the trade, global capital flows and environmental degradation, the revolution of the Information Age, epitomized by the cyberspace, as one of the contributors to the factors that undermine state sovereignty in the classical sense.

Besides Wriston, Saskia Sassen, the renowned leftist political scientist and sociologist, should also be added to this group, as well. As previously told, Perritt's article (which is reviewed and categorized under the next subheading) started off the debate regarding the relationship between state sovereignty and cyberspace, which, for the reasons stated, triggered an initial fervor about the topic in the 1990s that did not survive into the millennium. The studies regarding cyberspace was subjected to intense securitization and militarization, which left this field as a subject of the security studies and international relations, rather than a political science or sociology research topic. Perritt's article drew a powerful reaction from the neo-Marxist political scientist Saskia Sassen (1998), who focused on yet another aspect

of cyberspace and came up with counter arguments against the ones put forward by Perritt. Sassen (1998) takes into consideration "the architecture of the Internet" as she calls it, and brings about the discussion of public vs. private dichotomy regarding cyberspace, which is a deepened shot into the cyberspace studies back then. Criticizing the points and overall approach of Perritt's article while simultaneously accepting the credibility of his arguments that the Internet does not simply erode state sovereignty, Sassen (1998) choses to focus on the Internet's being "a contested space with considerable potential for segmentation and privatization" (p. 546-547). Sassen (1998) analyzes the question of the role of the private sector, focusing on the corporation-dominated architecture of the Internet:

> This is a particular moment in the history of digital networks, one when powerful corporate actors and high performance networks are strengthening the role of private digital space and altering the structure of public digital space, that is, the Internet. Digital space has emerged not simply as a major new theater for capital accumulation and the operations of global capital. (p. 547)

For Sassen, while democratic and open character of the cyberspace is still there, and though it has potential to limit the possibilities of the authoritarian and monopoly control, this does not necessarily translate into the strengthening of non-state actors vis-à-vis the states and eroding of state sovereignty. Sassen recurrently makes it clear that, with the establishment of the World Wide Web in 1993 and its large-scale commercialization in the second half of the 1990s, the cyberspace has been parceled out by private companies and it has left little proper place for the individuals and societies to eke out marginal existences within. Since the concepts such as firewalls, tunneling or encryption were not yet fully developed in their entirety at the time the article was written, Sassen views these concepts as factors that would drive out non-corporate elements out of the cyberspace. The punch line of

Sassen's analysis is that, excessive commercialization, far from strengthening the Internet's democratic potential, as Perritt also maintains, can threaten it.

The examples Sassen mentions to exemplify the commercialization process of the Internet, for instance, are the 1997 Aspen Roundtable on Electronic Commerce, an annual event, that brings together the CEOs of the main software and hardware firms, and similar private initiatives that regulate the Web or technical architecture of the Internet. It needs to be noted that Sassen does not ignore the cyberspace's potential for the development of free markets in the former centrally planned economies of Eastern Europe and the former Soviet Union (at least for a while). However, the article by Sassen locates itself at the opposite of that of Perritt by charging the latter with misreading some of the features of the cyberspace and confusing private digital space with public digital space. Surprisingly enough, this kind of analyses based on economical factors, corporation involvement and so on, like Sassen's piece, did not continue into the cyberspace studies in the field in the 2000s and other works handling state sovereignty and cyberspace, leaving Sassen's work a unique one. The economics-based cyberspace studies written thereafter chose to do so without delving into the concept of "sovereignty" and analyzed mostly the corporations, economical balances, the role of ICANN and cyber security markets only. Sassen's work is thus, coming from a political economic background, a special one.

Another study that directly and indirectly argues the cyberspace constitutes a platform that could undermine state sovereignty is the book by Milton Müller (2013), titled as *Networks and States: The Global Politics of Internet Governance*. The restriction tools such as filtering or censorship that are used by nation states are thought to strengthen a state's sovereignty but Müller challenges this argument by

basically claiming that cyberspace fosters new transnational institutions and cooperation. These novelties might all, for Müller, challenge state sovereignty eventually and he shows in his book how Internet governance poses novel and fascinating governance issues that give rise to a global politics and new transnational institutions. Müller (2013) argues that:

> The state, as political scientists insist, is still the predominant supplier of effective public governance and is still an immensely powerful institution. But there is a strong and persistent tension between state sovereignty, which is territorially bounded, and the nonterritorial space for social interaction created by networked computers. This tension puts pressure on the existing nation-centered institutional arrangements in communication and information policy. (p. 1)

For Müller (2013), the Internet "globalizes the scope of communication", "facilitates a quantum jump in the scale of communication", "distributes control", "grows new institutions" and "changes the polity", all of which has drastic consequences on the sovereignty of nation-states (p. 15).

One another significant study regarding cyberspace and sovereignty is the article by Forrest Hare, which bears the title "Borders in Cyberspace: Can Sovereignty Adapt to the Challenges of Cybersecurity?" (Hare, 2011) and, as its name suggests, tries to come up with analytical answers to this question stated in the title of the article. Based on these findings Hare (2011) arrives at a normative conclusion: "Assuming this paper successfully demonstrated the former case is more true than the latter, than regardless their exact physical location, the very existence of borders demonstrates a need for us to work together as international community to develop transnational solutions" (page unspecified).

A similar study to this article by Hare is an article by Goldsmith. Goldsmith, in his article "The Internet and the Abiding Significance of Territorial Sovereignty," scrutinizes the question whether the cyberspace might have any implications for the

territorial sovereignty of a state. Goldsmith (1998) argues that the regulation of the Internet is difficult for a couple of reasons. Firstly:

> because Internet information flows cross territorial borders without detection, and because Internet content providers can shift with relative ease the source of their information flows outside of any regulating territory, much of the content of the Internet is beyond the regulatory scope of any particular territorial sovereignty. (p. 478)

However, as the title of the article suggests, he argues that despite this difficulty in territorial regulation, it might be within the possibility of a nation to control it. It will just be difficult and might have an overall effect of eroding the sovereignty of the states in the long run. The article is a convoluted one and cannot be easily packed into one of the two groups.

The latest and most recent contribution to the debate is the study by Melissa Hathaway (2014), "Connected Choices." Reflecting where the debate has gone from its initial stages, Hathaway's study focuses on the dynamics of how the Internet is challenging sovereign decisions. She brings about a totally new discussion of the cyberspace and its effects on state sovereignty by approaching the topic from a global, country-based perspective. For Hathaway (2014), some countries are more prepared to have powerful presences in the cyberspace while some other could be totally weak, and the latter states might witness an erosion of sovereignty by the more cyber-powerful ones (p. 301). Hathaway describes these actions as competition for the cyberspace in a larger sense.

### 4.3 Studies arguing the strengthening of sovereignty by cyberspace

At the direct opposite of these works which, in a way or other, argue that cyberspace is a factor that undermines and erodes state sovereignty, another set of scholars preferred to view cyberspace as a platform that will contribute even more to

state sovereignty. The scholarly works in this camp conceive that cyberspace could and would be a tool of the governments in the modern world and thus strengthen their sovereignty practices. The firewalls, censorship and banning practices, monitoring and controlling devices employed by the nation states in the recent years, indeed demonstrated the credibility of this camp of thinking, in a clear way. If we completely ignore the fact that non-state organizations, individuals and hackers also profusely take advantage of the cyberspace, we see that it is a governmental tool nowadays. Russian cyber activities, for instance, making effective use of cyberspace and restricting the free speech, social and individual freedoms, render the country's cyber domain a "digital gulag" referring to the historical Russian concentration camps (Rothrock, 2014). A *Washington Post* article also focused on the same issue, by stating outright that "We may be the last generation to enjoy free Internet" and argued that:

> Edward Snowden's supporters have portrayed him as the champion of Internet freedom. But when senior European and U.S. experts privately discuss the future of cyberspace, their fear is that the Internet may be closing, post-Snowden, rather than opening. "We may be the last generation to take joy from the Internet," because of new boundaries and protectionism, as one American glumly put it. (Ignatius, 2014)

The study that triggered the debate between the two camps that are reviewed here can be said to be the article by Perritt. After Wriston published his article on *Foreign Affairs*, Perritt published his own article, titled self-explanatorily as "The Internet as a Threat to Sovereignty?" What Perritt includes in his article is, partly as a response to the main argument of Wriston's piece on *Foreign Affairs*, an analysis of the cyberspace as a political tool. Perritt argues that the Internet, rather than eroding the tenets of state sovereignty, has the potential to strengthen national and global governance, thus enhancing state sovereignty even more. Perritt (1998) challenges

the previously mentioned idea by asserting that the nation state governments can also use the cyberspace since "most of the new information technologies also offered sovereigns great potential to hold on to or even increase their power over their subjects" (p. 246). He exemplifies this by mentioning the wide use of technological advances such as cinema, radio and television by the twentieth century fascist and totalitarian regimes.

One of the central ideas in Perritt's article is that he views the "Internet as a threat to sovereignty" thesis as stemming from the realist understanding of national sovereignty and power, and that, these conceptions of sovereignty are already challenged by the liberalist approach. The realist approach, for Perritt, utilizes an abstract notion of sovereignty that is thought to be absolute and clear-cut, and if one bases one's arguments on this kind of "sovereignty" definition, then it sounds plausible that the Internet might constitute an undermining force for state sovereignty. For Perritt, there are enough reasons to think that the cyberspace is a medium that could undermine state sovereignty for a couple of distinctive characteristics of the cyberspace. First and foremost, "the most distinguishing feature of the Internet that makes it more threatening to sovereignty is that it is not susceptible to the same physical and regulatory controls as telegraph, telephone, radio, and television technologies" (Perritt, 1998, p. 246).

Another significant distinctive characteristics of cyberspace is that it also differs from earlier advances in information technologies since it "combines global reach with extremely low barriers to entry" which means that anyone with a laptop computer and Internet access is a full beneficiary of the cyberspace at an instant. For these reasons that Perritt rightly lists down and details, more analyzers wrote about cyberspace's undermining potential for the conventional sovereignty. These analysts

focused on the mind-boggling fact that, for the first time in history, at least for the first time so obviously, a medium is threatening the three historic functions of the state altogether, namely, providing national security, regulating economic activities and protecting and promoting civic and moral values, Perritt (1998) argues (p. 246). He then takes one step backwards from this debate and comes to the main argument of his article, which puts forward repeatedly that the cyberspace represents a powerful tool to strengthen national and global governance, enhancing what political scientists call "sovereignty." For Perritt, the cyberspace comprises a powerful tool for governments and effectiveness of the laws and thus increases the efficiency of the governing mechanism. Perritt (1998) focuses in this way on cyberspace as "a giant reservoir of legal models, judicial decisions, legal practices and advice on legal reform issues" (p. 246). The conception of sovereignty that the cyberspace is thought to foster is thus a "liberalist" one, for him, with the Internet strengthening rule of law, application of state regulation and the drafting of more efficient regulatory and legal mechanisms.

It must be noted that Perritt, for reasons unknown, does not mention in any way the control or surveillance mechanisms that are the most efficiently used cyberspace features by political authorities, most probably because the cyberspace comprised of only informative webpages and online platforms at the time the article was written. The security and control mechanisms that states use for the purposes of internal and external security such as firewalls, inspection tools or access control mechanisms, the factors requiring the usage thereof, were not yet available. Perritt also adds the issue of global governance of the Internet, arguing that the cyberspace has the potential to enhance global governance and international cooperation by constituting a global platform by nature, which requires the nation states to come

together and make political and economic agreements. For Perritt, this indirectly contributes to the "sovereignty" practices and capabilities of nation states. Oddly enough, he also finds cyberspace's "strengthening non-state actors" as an even more contributing factor to state sovereignty, a factor that he lists down together with "improving international security mechanisms" and "strengthening economic independence," both being the ways through which the cyberspace holds immense potential to enhance state sovereignty.

What Perritt theoretically argued in his article, echoed in the comprehensive book by Betz & Stevens (2012), namely, *Cyberspace and the State*. The book directly deals with the tools and techniques that the states use in the cyberspace, indirectly and frequently hinting that cyberspace strengthens state sovereignty by providing the states with novel cyber tools. Betz & Stevens provide a succinct, introductory level survey of global information technologies, certain risks, threats and opportunities inherent in these technologies, but it is quite quasi-theoretical in analytical substance and this renders the book's title too daring. Betz & Stevens, presenting a singular conceptual framework, tackle the diverse range of issues raised by the dependence on digital networks, considering how instantaneous global communications are challenging national & social orders and what shape these challenges might take as the cyberspace usage is getting wider and wider. The book, rather than arguing only one main argument, is a collection of the definitions and explanations for the concepts such as cyber power, cyber practices, cyber politics, and so on, namely the concepts regarding the state and the cyber. The book presents a singular, conceptual framework which is useful for initial thinking, but it can be said to be lacking any political case content or empirical basis. At the introductory chapter to cyberspace and state, the authors argue that:

> The simultaneity of cause and effect in cyberspace has obvious ramifications for the exercise of some forms of power: actions initiated in one location can have instantaneous effects in another, regardless of their geographical separation. While this allows state actors access to a greater range of globally distributed targets amenable to coercion of various forms, it also facilitates the reverse dynamic, in which spatially distant others – particularly those outside a state's immediate jurisdiction – can exercise power against the wishes of a state with little or no chance of being traced or interdicted by that state. (Betz & Stevens, 2012, p. 40)

In this quote from the book, Betz & Steven come closest to the main argument of this thesis and it can be said that it summarizes the primary argument of the thesis and the cases of it. It is true, obviously, but Betz & Stevens, in the further chapters of their book, focus more on the state practices in the cyberspace, which gives a larger picture of state sovereignty getting even more powerful. Betz and Stevens must be given the credit for not looking at the subject from just one single angle and noticing the importance of the cyberspace for both the nation states, and the non-state actors against them. Regarding state practices in the cyberspace, they add that:

> There are many other examples that could be used to illustrate how both liberal and authoritarian governments are pursuing forms of control over cyberspace in order to mitigate perceived threats against domestic sovereignty. In the West and elsewhere, terrorism is commonly invoked as the justification for doing so. (Betz & Stevens, 2012, p. 68)

This, Betz & Stevens argue, happens through numerous ways: "Attempts to control citizens' activities through the exercise of various forms of power in cyberspace have unsurprisingly, in turn, met with further resistance" (Betz & Stevens, 2012, p. 68). After stating this, the authors give two examples; one from China, the Chinese firewall practices, that this thesis handles in detail, and secondly, the physical cutting off of the Internet during the Egyptian mass protests in 2011. The authors differentiate between the types of sovereignty of nation states, just as this thesis has done, and try to look at the effects of the cyberspace on each

sovereignty type. However, all these sovereignty types are either not affected at all or end up with strengthening even more, since the states seem to be active on cyberspace themselves:

> The effect of cyberspace on domestic sovereignty is substantially a function of the tendency of cyberspace to ride rough-shod over governments' control over what passes across their borders. Even though cyberspace is a medium of information exchange, the information it carries is decoded as persuasive ideas and ideologies, and/or converted into capital in the form of goods and services. While the latter are pursued with vigour by states, the former are the object of equally robust attempts at repression. (Betz & Stevens, 2012, p. 72)

About a decade ago, another study in this same camp was published, within the time interval when many state practices in cyberspace took hold. The book by Jack Goldsmith and Tim Wu (2006), namely, *Who Controls the Internet?: Illusions of a Borderless World,* focuses on state responses to the Internet's challenge to national sovereignty. The main argument is that national governments, through coercion and control over local intermediaries, still exert regulatory control in the realm of the cyberspace. Thus, Goldsmith and Wu question the popular notion that the Internet is erasing national boundaries and rendering geography obsolete. Goldsmith and Wu explore three main arguments, first of which is that, the cyberspace is a medium like any other, and national governments continue to exercise control over the Internet by enforcing state law. Secondly, in spite of the continued globalization, the geography and the national governments retain their central importance over the Internet and thirdly, despite the popular belief, an increasingly "bordered" Internet might be a positive development.

Similar to the study by the Goldsmith & Wu, Evgeny Morozov, in his controversial and groundbreaking book *The Net Delusion*, published in 2011, contradicts what he calls the "cyber-utopianism," the fascination with the cyberspace

holding that it is going to be a platform for emancipation and democratization of the societies vis-à-vis the nation-states. He rather boldly demonstrates how the digital tools so useful to citizens in free society are also employed by tech-savvy dictators, police states and autocrats to disseminate propaganda and to track and arrest dissidents online more easily than ever. By providing numerous examples of how authoritarian regimes have used technology to track people, Morozov sets up a giant edifice of how the cyberspace might contribute to the sovereignty of states. Challenging the optimism regarding the cyberspace, Morozov (2011) states that:

> Failing to anticipate how authoritarian governments would respond to the Internet, cyber-utopians did not predict how useful it would prove for propaganda purposes, how masterfully dictators would learn to use it for surveillance, and how sophisticated modern systems of Internet censorship would become. Instead most cyber-utopians stuck to a populist account of how technology empowers the people, who, oppressed by years of authoritarian rule, will inevitably rebel, mobilizing themselves through text messages, Facebook, Twitter, and whatever new tool comes along next year. (The people, it must be noted, really liked to hear such theories.) Paradoxically, in their refusal to see the downside of the new digital environment, cyber-utopians ended up belittling the role of the Internet, refusing to see that it penetrates and reshapes all walks of political life, not just the ones conducive to democratization. (p. xiv)

His other chapters all compile and analyze the methods that the states use, such as the NSA's secret monitoring of the cyberspace users in the US or the world in general, together with the other states' practices, which are even more in violation of the privacy of the users. Morozov's take on political powers of the cyberspace is extremely detailed and comprehensive; however, trying to quote from his work in this thesis could take too much space.

Quite reminiscent of Morozov, another study, though surpassed in scope by Morozov's work, is the one titled as *Black Code*. Published by Ronald Deibert (2013), the book takes into its center the surveillance and anti-privacy practices by the nation-states in order to increase their sovereignty in and out, meticulous

examination of the “malicious threats that are growing from the inside out” on the Internet and which “threaten to destroy the fragile ecosystem we have come to take for granted.” Delivered like a novel or a great narrative at times, *Black Code* provides first and secondhand accounts on a wide variety of conflicts in cyberspace. China's cyber espionage of the exiled Tibetan government through the DarkComet RAT and koobface, the Russian-based botnet created for the sole purpose of enabling Facebook click fraud are just examples of the practices of the nation states in the cyberspace. The diversity and quantity of cyber methods that the nations use are numerous, and the book tries to touch them mostly. However, it looks more like a compilation of them rather than an academic profound analysis.

As can be seen from the entries in this camp, the scholars focused on the immense potential that the cyberspace holds for the state sovereignty. Almost all of the scholars preferred to focus on the actively-conducted empirical state practices in the cyberspace such as firewalls, censorship, monitoring and other similar methods. Morozov, among the scholars in this camp, is the one that brought up the issue of regimes as an independent variable in his analysis. The cyberspace renders the liberal regimes more liberal and authoritarian regimes more authoritarian, argues Morozov. Rather than treating all the states similarly wholesale, he tries to go deeper into the regime practices and ideologies.

One more study in the cyberspace-sovereignty relationship debate, with its profound and recent arguments, deserves to be handled outside of these two camps that are reviewed about. The study by Trachtman, arguing quite similar points to the points of this present thesis, stands out among others, and, since it cannot be packed easily into either of the two camps above, needs to be reviewed singularly.

## 4.4 Beyond eroding or strengthening: Trachtman

Soon after the kindling of the debate regarding sovereignty and cyberspace, Joel Trachtman (1998) contributed to it with a legal-based treatise in which he analyzed the cyberspace with better analytical profundity and significant points. Trachtman opposes the idea of the cyberspace being a total game-changer and views it more like another platform that deepens the relationship between the state and non-state actors. He promises to lay down "the things that cyberspace actually changes and out ability to predict the results of these changes" (Trachtman, 1998, p. 561). Arguing quite rightfully that the cyberspace basically leads to "new allocations of power both to the state and non-state entities" (Trachtman, 1998, p. 561). Trachtman approaches the concept of sovereignty as a problem of institutional competence. Distinguishing between "conclusory sovereignty" and "contingent sovereignty," Trachtman announces the death of the former, since it has a strict and hard definition of sovereignty practices and principles.

The most significant idea Trachtman (1998) puts forward in his treatise is that "the cyberspace is neither clearly sovereignty-demeaning nor clearly sovereignty-preserving: the cyberspace today is neutral in the contention over the powers of the state" (p. 565). He adds that "[t]hose who purport to tell us whether cyberspace will, in the course of time, demean or enhance the powers of the state must fail, as this question cannot be answered in general or in advance, but must be answered as we evaluate and build particular institutions over time" (Trachtman, 1998, p. 565). In this way, Trachtman sees the cyberspace as yet another platform where the game of sovereignty is played out between the state and non-state actors. Since the cyberspace is a space which not only facilitates private activity, but also facilitates government activity, it "not only strengthens the tools of government, but it can also

strengthen the legitimacy of government through heightened transparency and democracy" (Trachtman, 1998, p. 565). Trachtman also adds, though slightly and indirectly, the control and surveillance mechanisms facilitated by the cyberspace, which would have an overall effect of slightly increasing state sovereignty, as we know it.

One of the most noteworthy ideas Trachtman's article puts forward is that, he sees the "territoriality" principle of sovereignty, meaning that a state is sovereign over a specific portion of physical space, might be undermined by the non-spatial nature of cyberspace, which Trachtman sees as a problem of archaic understanding of jurisdiction. This manifests itself in the form of problems regarding the regulation of the cyberspace, both national and international. The cyberspace, then, rather than eradicating the state sovereignty as we know it, "simply accelerates the realization of this fact" (Trachtman, 1998, p. 570), namely, the perceptual problems of the territoriality principle of jurisdiction (and thus sovereignty.) Rather simply, shortly and boldly, Trachtman (1998) asserts that "[t]he rise of cyberspace will not destroy the state" (p. 580) and the cyberspace strengthens the powers of the state as well as demean them (p. 580).

Trachtman's points and arguments seem to be the most advanced ones in the literature of cyberspace and sovereignty. They are also the most akin to the main argument of this article, though Trachtman lacked the examples of technical and technological advances to back up his arguments at the time. In this regard, this present thesis builds upon the literature with the most recent advances in the 2000s and 2010s, in a way supporting Trachtman's assertion that the cyberspace, rather than merely eroding or strengthening state sovereignty, constitutes a space to do both.

This chapter compiled and analyzed the literature regarding the cyberspace and sovereignty. As can be seen from the chapter itself, this literature can be basically divided into two academic standpoints, and one conciliatory group of scholars that merge the arguments of the two. The first group of scholars basically argue that the cyberspace is going to constitute a platform, which, in one way or other, will erode nation-state sovereignty. The group of scholars here, to which the first social scientist analyzer of the cyberspace also belong, hold that, through a set of different mechanisms, the cyberspace eventually might erode the absolute state power. The first way this could take place is that, since cyberspace removes the boundaries to gather and to reach to information, it could constitute a place where non-state actors mobilize against the state sovereignty and power. Other scholars in the group, in keeping with their leftist tendencies and the spirit of the beginning of the 1990s, focused more on the strengthening of the private sector and businesses through the cyberspace, since this domain's research, development and marketing are conducted by the private sector. The next chapter, with its empirical cases and findings, attempts to explore and empirically materialize the theoretical arguments of this chapter regarding the literature on the cyberspace and sovereignty.

After looking at the literature that analyzes the cyberspace and nation state sovereignty issue, it is now the time to look move on to the cases of the thesis and analyze them to see which arguments of this literature can be uphold and which ones cannot.

# CHAPTER 5

# CASE STUDIES:

# SOVEREIGNTY STRENGTHENED, SOVEREIGNTY ERODED

This chapter, building on the previous ones, analyzes the cases that support the main argument of the thesis. As can be remembered from the previous chapters, the main argument is that cyberspace, rather than solely strengthening or eroding the nation-state sovereignty, just adds one more field on which the battle between the nation-states and non-state actors can be fought. There are many cases that erode the nation-state sovereignty and many others in which sovereignty of a state can be said to strengthen in either short or long run. The cases listed here briefly look at the history of the case, in which way the cyber incident had an affect of the sovereignty of the state in question and in which cyberspace layer (according to the Clark's 4-layered cyberspace model) the incident took place.

The cases are organized as subtitles and are kept as detailed as possible, and as simple as an average reader can read and understand, since the technical details for each of them are available yet irrelevant for the purposes of the thesis. Some of the cases involve a nation-state-to-nation-state cyber case such as the Stuxnet case which was perpetrated by the USA and tested in Israel; while the RedHack case includes cyber attacks conducted by a hacker group against a nation-state, Turkey. All the cases might greatly differ from each other in terms of the actors or the extent of the case; however, they include at least one aspect that touches the sovereignty of a nation state in some way. All the cases make clear in the end whether the sovereignty of the specified nation state concerned is strengthened or eroded, using

the sovereignty operationalization scale put forward by Ghani, Lockhart & Carnahan and reviewed previously in detail in the sovereignty chapter of the thesis.

At this stage one point must be highlighted. When one has a look at the number of cases in which sovereignty is eroded and the number of those in which sovereignty is strengthened, one realizes a huge discrepancy between them. In other words, the number of cases where sovereignty of a state is claimed to be eroded is six, while the number of those in which sovereignty is strengthened is just two. The reason for this apparent difference is that, the main actor in the cases where state sovereignty is strengthened is the same: it is always the state itself. For this reason, two cases were quite enough to show a situation in which a state's sovereignty (mainly over its subjects) got strengthened due to its efficient use of cyberspace. On the other hand, the number of cases in which the state sovereignty is claimed to be eroded is six, a relatively greater number. In these cases, some of them exemplify a situation in which the sovereignty of a state gets eroded due to an external source, such as another state (such as the cases Stuxnet and Sony Entertainment Co. Hacking in which the sovereignty practices of Iran and the US, respectively, got a negative impact). Yet some other cases are those in which the source of the erosion of sovereignty is internal, a subject of the sovereign; and the sovereignty of a state gets eroded due to the cyberspace use of such an internal source. For instance, in the case of RedHack, the source of the sovereignty erosion is RedHack, a hacker group, and in the case of the Egyptian Revolution that took Mubarak government down, the source of the sovereignty erosion is the Egyptian people itself, not a specific hacker group. This is basically the main reason of the seemingly great difference between the numbers of two groups of cases.

First group, the cases under the subtitle Sovereignty Eroded, consists of the six cases in which the sovereignty of a state is eroded due to the use of cyberspace.

## 5.1 Sovereignty Eroded

### 5.1.1 Bitcoin

Cyber methods that might erode nation state sovereignty include one feature regarding the monetary sovereignty of modern states. In addition to the more political and more power-related factors above, bit-coin must be added to this list, since, for the first time in history, a currency that does not bear the imprint of a nation state is in use. Bit-coin, based on a specific cyber "mining" process to produce, can be converted into US dollars and other currencies at certain rates, is already used in transactions in cyber markets, and most astonishingly, is not subject to any central bank of any nation.

One of the most basic tenets of a sovereign nation state is its monopoly over the economic means and activities that function within its borders and arguably the first and foremost sign of a sovereign nation state is to print or gild its own money. Actually, money is the most significant and direct indicator that a state is "sovereign." After the use of actual gold or coins, the paper money came into human use, printed by sovereign states. For instance:

> the dollar is valuable not because it's as good as gold, but because you can buy goods and services produced in the United States with it—and, crucially, it's the only form the US government will accept for tax payments. Among the Federal Reserve's many functions is allowing the issuance of just the right quantity of dollars—enough to keep the wheels of commerce well greased without slipping into a hyperinflationary crisis. (Henwood, 2014)

Bitcoin, the virtual currency that came into widespread use in the recent years is different, though. With Bitcoin, trading is done through exchanges, and there is no central state authority over the production or transmission of this online currency.

Figure 8 illustrates the timeline of the history of Bitcoin's development and use.

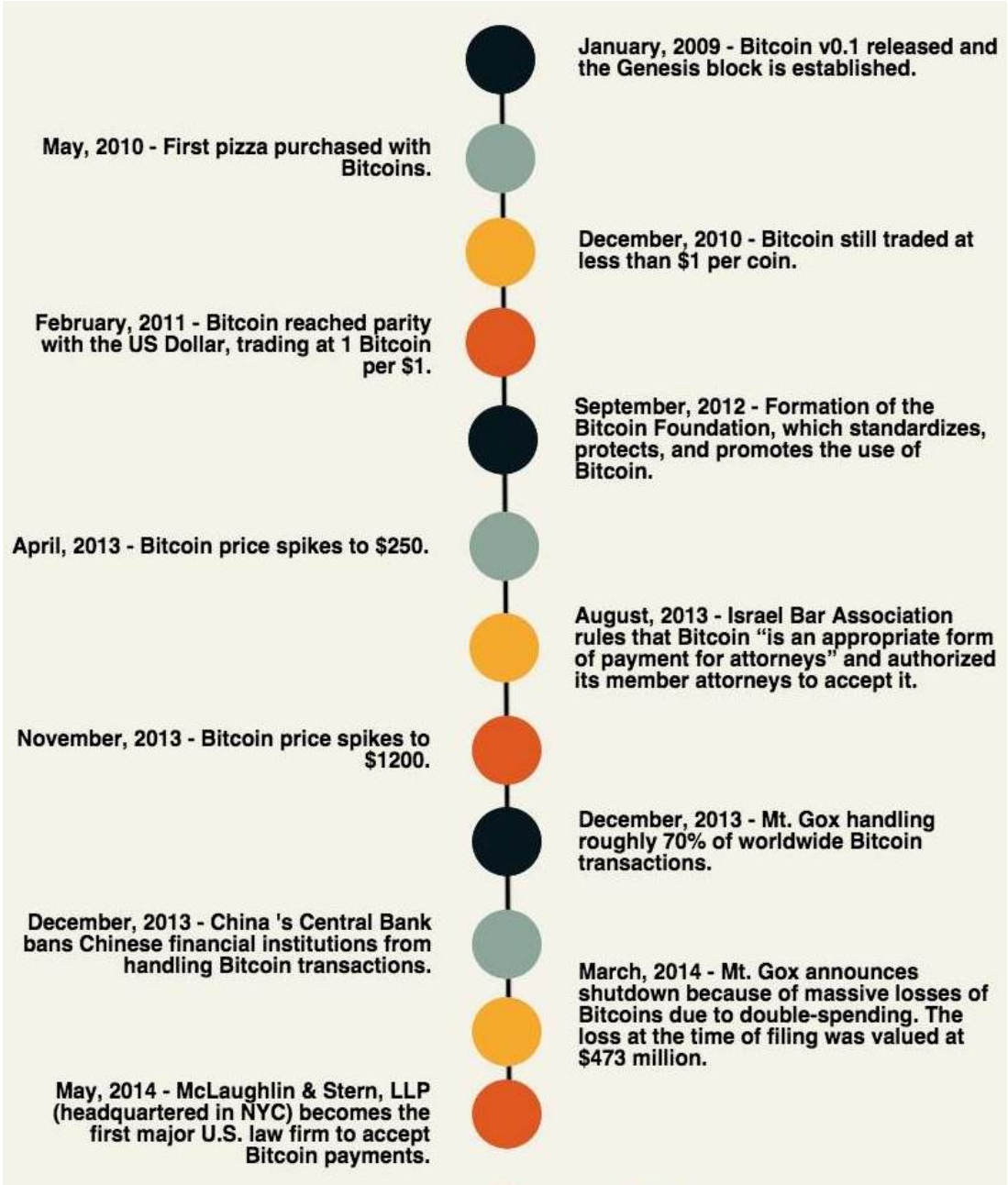


Fig. 8. History of Bitcoin (Source: Gunst, 2015)

Regarding Bitcoin, Federal Reserve chair Janet Yellen said right after the Mt. Gox collapse, that the Fed lacked the authority to regulate Bitcoin because it's outside the banking system (Rushe, 2014). Similarly, the Danish central bank stated in a press release: "Bitcoins are not money in a proper sense as there is no issuer behind them. Instead, bitcoins display the characteristics of a commodity to which users attach value. Unlike precious metals such as gold and silver, bitcoins have no actual utility value, bearing closer resemblance to glass beads" (Danmarks Nationalbank, 2014).

But, how does Bitcoin work? How can it reach the effectiveness of the currency of a state? Figure 9 illustrates the diagram of the Bitcoin's functioning.

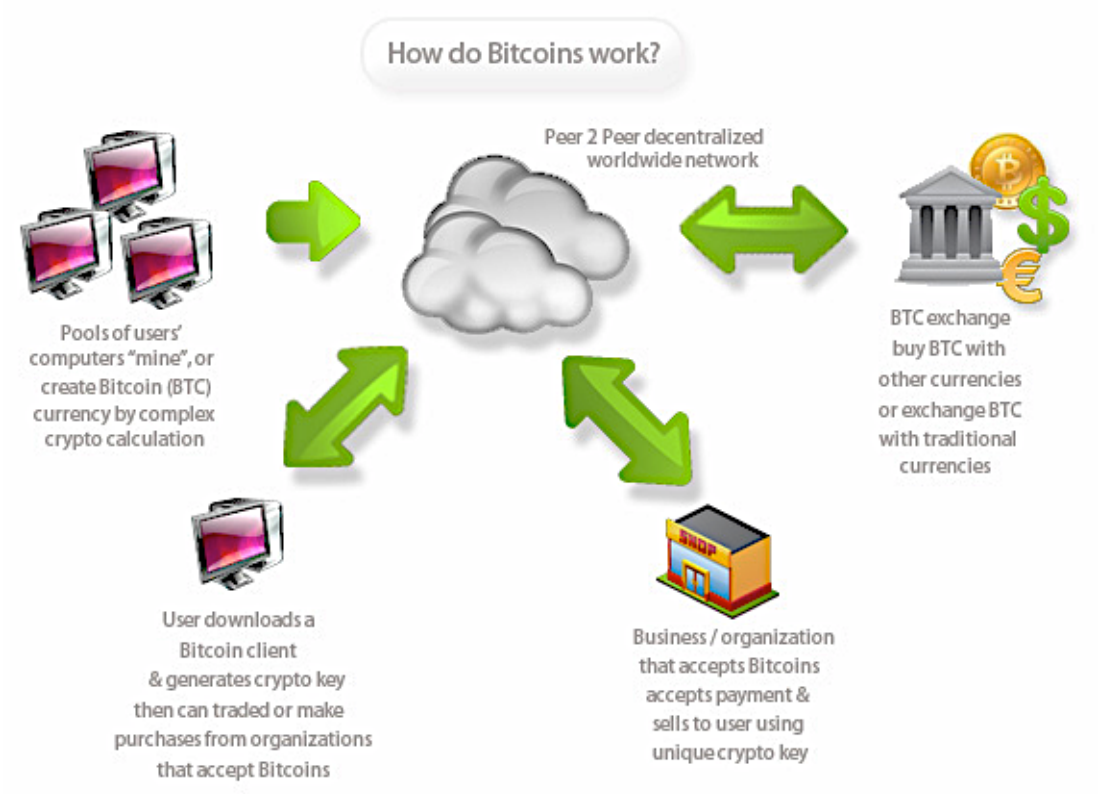


Fig.9. How do Bitcoins work? (Source: Bitcoin Bank GL, n. d.)

The first dimension of the Bitcoin flow is the computer systems that the Bitcoins are created, or rather, "mined" by constant calculation. One such computer pool where Bitcoin is mined can be seen in Figure 10.

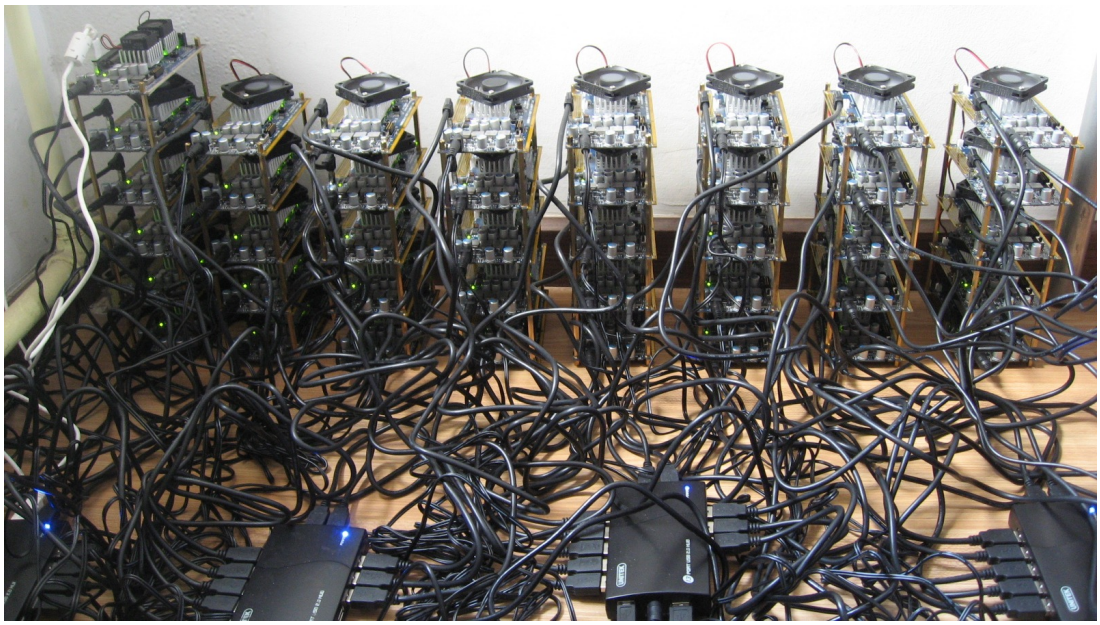

Fig. 10. A Bitcoin "mining" computer system (Source: Alluned, n.d)

The debate regarding the political control of the Bitcoin and whether the Bitcoin will flourish and be a legitimate currency or turn into a temporary pastime habit took hold in the recent years. For instance, two Goldman Sachs economists, Dominic Wilson and José Ursua, largely agreed with the Danish evaluation mentioned above. Their comment regarding the use of Bitcoin is that "We would argue that Bitcoin and other digital currencies lie somewhere on the boundary between currency, commodity and financial asset. Our best definition would be that it is currently a speculative financial asset that can be used as a medium of exchange" (Shieber, 2014). But they also make an important point: the peer-to-peer technology behind Bitcoin could become a model for moving money around without third-party verifiers, like banks (Shieber, 2014).

Improvised money systems that could challenge state sovereignty and monopoly over the money-producing tenet of states, from a historical perspective, has always been a dream of the extreme rightist groups, who believe in the absolute superiority of the market forces. In a 1976 paper, Friedrich Hayek (1976) argued for

allowing multiple currencies to circulate within individual countries; such a competition could ultimately lead to the use of the soundest currency, and put a check on the attempts of the governments to inflate pressures on the market, thus no fiscal or monetary stimulus by the government authorities. However, since the virtual currencies like Bitcoin lack regulation and some sort of insurance scheme, the scholars studying them also think that they will never be able to establish themselves as valid currencies.

The fear over the lack of governmental control over the use and production of the Bitcoin grew to such a level that the US Senators felt obliged to submit a letter to the US Senate regarding the issue. They cited in their letter some policy concerns, including a Texas case in which a man was charged with running a bitcoin-related Ponzi scheme and a May Government Accountability Office report that said the use of virtual currencies could lead to lost tax revenue (Tracy, 2013). “As with all emerging technologies, the federal government must make sure that potential threats and risks are dealt with swiftly; however, we must also ensure that rash or uninformed actions don’t stifle a potentially valuable technology,” Messrs. Carper and Coburn wrote in their letter, which was addressed to the Department of Homeland Security, the Federal Reserve, the Securities and Exchange Commission, the Commodity Futures Trading Commission, the Department of Justice and the Treasury Department (Tracy, 2013). In order to regulate the use of Bitcoins, the US treasury classified Bitcoin as a convertible decentralized virtual currency in 2013 and the Commodity Futures Trading Commission, CFTC, classified Bitcoin as a commodity (rather than a currency) in September 2015.

The real problem regarding the alleged loss of governmental sovereignty and control over the virtual currencies has to do with the definition of currency that is

currently used in the governmental circles. For instance, the Treasury Department's definition of currency is the coin and paper money of the United States or of any other country that is designated as legal tender and that circulates and is customarily used and accepted as a medium of exchange in the country of issuance. Currency includes US silver certificates, US notes and Federal Reserve notes. Currency also includes official foreign bank notes that are customarily used and accepted as a medium of exchange in a foreign country (Legal Information Institute, n.d.).

The decentralized nature of Bitcoin that defies the governmental control has attracted the attention of regulators as well. According to scholars, the same qualities that make Bitcoin attractive as a payment system "could also allow users to evade taxes, launder money, and trade illicit goods" (Brito & Castillo, 2016, p. 2), thus eroding the total sovereignty of a nation state over its economic functions. When one delves more into the Bitcoin issue, one sees that there is good reason to think that such virtual currencies will eventually erode state sovereignty. The first and foremost reason for this is that "[c]urrent law and regulation does not envision a technology like Bitcoin, so it exists in something of a legal gray area. This is largely the case because Bitcoin does not exactly fit existing statutory definitions of currency or other financial instruments or institutions, making it difficult to know which laws apply and how" (Brito & Castillo, 2016, p.2). Secondly, there are obviously some areas and related questions that arise together with the usage of Bitcoins. According to a detailed study conducted by the FBI, the lack of state control (and thus erosion of state sovereignty) will be visible on various fields related to the use of Bitcoins. The list entails some entries that might seriously affect a nation state's most basic control mechanisms. For instance, the first character of the virtual non-controlled currencies could render them effective "to purchase illicit goods" (FBI, 2012). The unclassified

document by FBI states that “The FBI assesses with medium confidence that, in the near term, cyber criminals will treat Bitcoin as another payment option alongside more traditional and established virtual currencies such as WebMoney, which they have little reason to abandon” (FBI, 2012). The technical analyses on Bitcoin all highlight the anonymity provided by the Bitcoin system for the users of this virtual currency. It is possible to create and use a new Bitcoin address for each incoming payment on the logic of the Bitcoin system.

Secondly, Bitcoin leads to “decentralized authority vulnerabilities” (FBI, 2012) since there is “no anti-money laundering software or monitoring capabilities to identify suspicious monetary patterns”, “no identification of account owners or their actual location” and “no historical records of transactions associated with real world identity” (FBI, 2012). Due to these reasons, law enforcement authorities cannot target one central location or company to control this currency, which is a serious blow to the monetary sovereignty of a nation state.

Thirdly, “money laundering” is stated as a serious problem regarding the use of the Bitcoin. It is stated in the document that “the FBI assesses with low confidence that malicious actors will exploit Bitcoin to launder money. The confidence level is based on observed criminal activities, investigations, and prosecutions of individuals laundering money through other virtual currencies, such as e-Gold and WebMoney” (FBI, 2012). Fourth concern regarding the use of Bitcoins is more about “the rule of law” characteristic of a sovereign state. Theft of Bitcoins is a problem in the face of which it is not possible to sustain governmental control. The FBI document “assesses with high confidence, based on reliable industry and FBI reporting, that criminals intending to steal bitcoins can target and exploit third-party Bitcoin services and an

individual's Bitcoin wallet, principally because there is no central Bitcoin server to compromise" (FBI, 2012).

After looking at the general features of the Bitcoin, we can now have a look in what ways the Bitcoin can undermine the sovereignty of states. For this purpose, the sovereignty operationalization scheme by Ghani, Lockhart and Carnahan will be used. Table 2 illustrates the points where the sovereignty of the US or any other state might be negatively affected. It should be noted that throughout the following cases, asterisk (*) is used to denote the points which might be negatively affected, and a plus sign (+) is used where the sovereignty of a state might be strengthened.

Table 2. Sovereignty Operationalization of the Bitcoin Case

| | |
|---|---|
| Legitimate monopoly on the means of violence | * |
| Administrative control | * |
| Management of public finances | * |
| Investment in human capital | |
| Delineation of citizenship rights and duties | |
| Provision of infrastructure services | |
| Formation of the market | * |
| Management of the state's assets (including the environment, natural resources, and cultural assets) | * |
| International relations (including entering into international contracts and public barrowing) | |
| Rule of law | * |

As Table 2 illustrates, the monetary sovereignty of the nation states are at stake due to the possible widespread use of virtual currencies like Bitcoin, as they are not subject to the monetary authorities.

Firstly, it can be undoubtedly argued that the legitimate monopoly of a state over the means of violence within its borders is likely to be eroded. The reason for this is that, Bitcoins, since they can be sent from any source to any destination with anonymity and free from any legal control, might be used for trading weapons and

other mass destruction tools on underground markets. The FBI study regarding Bitcoins specifically refers to this issue, as seen from the above remarks. Two basic tenets of the sovereignty of nation states, as indicated by Ghani, Lockhart and Carnahan, are also at stake due to the use of Bitcoins, namely, "administrative control" and "management of public finances" powers of the sovereign states. As explained by Ghani, Lockhart and Carnahan, the administrative control refers to "the existence of a coherent set of rules that determine the division of responsibilities horizontally and vertically across functions of the state and between hierarchical levels; the recruitment of civil servants; the spatial and functional division of administrative roles; and flows of resources and based on this definition, the functional administrative role of the monetary institutions in a given nation state is eroded due to the fact that they cannot conduct their routine checks on the monetary issues.

Secondly and similar to the previous article, "[s]ound management of public finances in today's interdependent world is probably the most critical indicator of the autonomy of a state. No state can be sovereign while it relies on an external source to fund its ongoing operations" (Ghani, Lockhart & Carnahan, 2005) and Bitcoin renders this function of a sovereign state fully or partially unfunctional. Formation of the market and management of the state's assets are two functions of a sovereign state as well, and they are harshly affected to the use of Bitcoin, as stated in the study by FBI. The state loses its grip on the markets due to the very fact that the currency used on some trades are fully outside of the state control.

The last tenet of a sovereign nation-state according to the operationalization scheme of Ghani, Lockhart and Carnahan is the rule of law and it means the upholding and maintaining of an order by the nation state as it sees fit. Due to the use

of a non-governmental currency, the non-state actors might easily enter into illegal trade and harm the rule of law, both within a country and internationally. This serious problem is stated in the study paper by FBI in 2012 above. All in all, there are obvious enough reasons to suspect that Bitcoins, and other virtual currencies, are an antidote to state sovereignty and might be expected to erode state sovereignty both in short and long term.

### 5.1.2 2014 Russian Dominance of Ukrainian Cyberspace

It is no wonder that Russia is a state that invests vastly and continually into increasing its cyber arsenal and cyber power in general, because of the fact that, for reasons already mentioned, cyberspace is a platform in which the states can easily challenge Western-dominated international order. The countries that host some of the most advanced cyber capabilities (outside of the Western camp itself) are Iran, China, Russia and North Korea, and evidently these countries have either ideological, political, historical or economic grievances (or a combination thereof) with the consolidated, Western-dominated international order, and they are also the ones in which governments support some sort of cyber command to undertake cyber activities against opponent countries. The perpetrator cyber groups located inside these countries might be some underground hacker groups supported, or turned a blind eye, by their governments and sometimes they are members of an outright official state unit, as in the case of China (Can, 2014b).

Russia is trying to enlarge its sphere of influence both through hard and soft power, attempting in every way possible to break or disrupt the influence of the Western camp, and now cyberspace is the new domain where we witness its similar disruptive efforts. Russia deliberately ignores the hackers located within its borders who are perpetrating some of the cyber attacks against Western countries, sometimes

out of ideological motives and sometimes in pursuit of sheer economical gain (Can, 2014b). Indeed, this Russian cyber-irredentism is so visible in the cyberspace that "[i]ndividuals and groups in Eastern Europe, particularly in Russia and Russian-speaking countries, are responsible for a fifth of all cyber-spying incidents in the world, according to a global study of data breaches recently released by Verizon" (Harris, 2014).

The case of Russia illegally hacking other nation states is not restricted to the Russian-Ukrainian conflict either and in 2008 Russo-Georgian War, Russia was able to use cyber methods against Georgia. In 2008, Russia and Georgia engaged in armed conflict over two republics, South Ossetia and Abkhazia that are both located in Georgia and backed by Russia in terms of their independence. Russia backed the separatists and eventually launched a military campaign. In the days and weeks before Russia's direct military intervention into Georgia, hackers originating from Russia attacked key Georgian information assets. Russia capitalized on the fact that Georgia did not have its own Internet exchange point (IXP) and was therefore reliant on Armenia, Turkey, and Russia for nearly 70% of its Internet exchange capacity (Rivera, 2014). As a result, this allowed Russia to exert control over Georgian web activity at a few choke points, which in turn allowed Russian cyber forces to destruct some Georgian government websites. In Georgia, Internet connectivity was down for extended periods of time and official government websites were hacked or completely under the attacker's control. The cyber attacks also targeted internal communications and news outlets and they were thus severely disrupted. All of the above harmed the ability of Georgian military commanders to coordinate defenses during the initial Russian land attack, which is actually itself a cyber case that can serve the purposes of this chapter, since the sovereignty of the Georgian state was

severely eroded due to the lack of information technology connectivity problems both inside and outside the Georgian military.

The events leading up to the pro-Russian unrest and annexation of Crimea by Russia need to be understood firstly in order to truly conceive the Russian cyber role. Ukraine got into a sort of chaos when President Viktor Yanukovych refused to sign an association agreement with the European Union in 2013, which led to an organized political movement that demanded closer ties with the European Union. But the immensely pro-Russian eastern and southern provinces started large-scale protests in favor of Russia and with Russia interfering in, the Crimean peninsula was annexed by Russia and some eastern Ukrainian provinces were briefly occupied by Russian forces.

However, the real issue regarding this conflict that concerns this thesis is the Russian cyber activities in parallel with the ground insurgencies. "As economic sanctions have punished Russia for its aggression in Ukraine, the Russian leader has used a combination of regular and irregular cyberforces that are now jockeying for resources and accolades from Moscow," wrote Bloomberg, and added "'They're being successful. If you're doing something that's working, you're going to keep doing it,' said Lewis, now chief collection and intelligence officer for LookingGlass Cyber Solutions Inc., based in Arlington, Virginia" (Riley, 2015).

The same cyber threat that Russia used against Georgia was once again a threat in the case of the Crimean Annexation. Ukraine's Crimean Peninsula, while not as technically isolated, was similarly vulnerable as Georgia, because of the Internet exchange points. Ukraine had various IXPs located within itself, however only one was located in Crimea. Thus the cut-outs against this IXP meant the isolation of the Crimean peninsula from other Ukrainian territories and a complete cyber victory for

Russia in the region. It must be noted that this cyber attack took place on the "physical layer of cyberspace", according to the classification of Clark in the cyberspace chapter of this thesis.

The Russian attacks against the Ukrainian cyberspace took place in other cyberspace layers as well. The information layer of the cyberspace also went under Russian attack. The hackers backed by Kremlin attacked Ukrainian sites with relative ease and posted false news to mislead the public, a common Russian propaganda tool. As an example, Russian cyber forces attacked the website of the Ukrainian National Guard just hours after the ceasefire went into effect on midnight February 14. They also posted a news item claiming that "the [Ukrainian] Right Sector leader vowed to continue its attack on the besieged town of [Russian] Debaltseve despite the ceasefire." Immediately after this, the pro-Kremlin websites like *Russia Today* and *Sputnik* took this false news as Ukraine's breaking the terms of the ceasefire (Maheshwari, 2015).

The first days of the conflict witnessed some other Russian cyber [or, in this case, electronic warfare] attacks, as well. Pro-Russian hackers physically disrupted the Ukrainian media and telecommunications networks, which prevented the Ukrainian government from reaching to their constituents about what was going on in the Crimean Peninsula and this totally hampered the ability to mobilize counter-forces against the pro-Russian forces, according to the Ukrainian military reports. It must be noted that this took place also on the "physical layer" of the cyberspace (Martin-Vegue, 2015).

One Russian hacking group worked effectively during the Ukrainian conflict. The cyber-group called Cyber Berkut, when the NATO officials arrived in Kiev to discuss the ongoing conflict, started out its cyber attacks against most of the

Ukrainian governmental websites, preventing the access to them for days. The cyber group also stated "If NATO cannot protect their resources, the protection of personal data of ordinary Europeans cannot be considered," in an open web explanation. In later weeks, the group also launched DDoS attacks against media sites that it accused of spreading "fascist and nationalist propaganda," which apparently means pro-Ukrainian or not sufficiently pro-Russia. Five general-interest Ukrainian media sites were targeted and also 700 mobile phones used by Ukrainian governmental officers were allegedly blocked by the same Russian cyber group (Shwartz, 2014).

The attacks against the physical cyber infrastructure of Ukraine continued in other fields as well. While the conflict was going on in the Crimean peninsula, late on 28 February 2014, unknown people seized several telecommunications nodes in Crimea. In view of this fact, Ukrtelecom officially reported that the company had lost the technical capacity to provide connection between the peninsula and the rest of Ukraine and probably across the peninsula too. Ukrtelecom was literally forced to make an open and official statement to its users, which included:

> The unknown individuals damaged the fibre backbone cable of Ukrtelecom. As a result, there are almost no services of fixed telephony, Internet access and mobile communications TriMob provided in the territory of the Crimea. Ukrtelecom states that communications services are VITAL to sustain essential support systems in the peninsula including first aid, fire and rescue services. (UkrTelecom, 2014)

According to the reports, in March 2014, a Russian cyber weapon called Snake or "Ouroboros" led to chaos on Ukrainian government systems (Ross, 2014). In addition, in October 2014, Russian hackers exploited a bug in Microsoft Windows and other popularly-used software to spy on computers used by NATO, the European Union, Ukraine and companies in the energy and telecommunications sectors, according to cyber intelligence firm ISight Partners (Finkle, 2014). According to the

more recent reports, a Russian hacking group Sandworm or the Russian government were behind the Ukrainian power grid malware attack in December 2015, as the latest reports in the aftermath of the Crimean conflict and its total annexation.

After looking at the case of the Russian dominance of Ukrainian cyberspace and how it affected the Ukrainian sovereignty, we should apply the sovereignty operationalization scheme by Ghani, Lockhart & Carnahan that was reviewed in the sovereignty chapter of this thesis. The ten functions of a sovereign state and which ones of them can be said to be affected in this case gives us the Table 3. It should be noted that the table illustrates the effects on Ukraine's sovereignty tenets, and, the asterisk signs (*) on the table show the areas where the Ukrainian sovereignty got seriously (and negatively) affected.

Table 3. Sovereignty Operationalization of the Russian Dominance of Ukrainian Cyberspace

| | |
|---|---|
| Legitimate monopoly on the means of violence | * |
| Administrative control | * |
| Management of public finances | |
| Investment in human capital | |
| Delineation of citizenship rights and duties | |
| Provision of infrastructure services | * |
| Formation of the market | |
| Management of the state's assets (including the environment, natural resources, and cultural assets) | * |
| International relations (including entering into international contracts and public barrowing) | * |
| Rule of law | * |

As it can be seen from the processes and points indicated on Table 3, the Russian cyber attacks, backed by the Russian state itself, had a negative influence on the Ukrainian sovereignty. When these points are considered, in our current case, the Ukrainian sovereignty can be said to be seriously eroded due to the following points.

Firstly, the Crimean peninsula was physically occupied and annexed by Russia, with the help of cyberspace, which brings us to the conclusion that cyberspace had a serious effect on the legitimate means of violence. In addition, the fact that Ukrainian National Guard's website was hacked and fake news were posted, and as a result of this, Ukraine was shown as breaking the terms of the ceasefire, is a clear violation of the Ukrainian cyberspace.

Secondly, the rule of law in the territory and Ukrainian administrative control in the region were severely disrupted, since the peninsula and the rest of the country was literally cut. The fact that Ukrainian official sites were hacked and some false information were posted on them shows us an erosion of the Ukrainian sovereignty in terms of administrative control and the rule of law as. The fact that Ukrainian media and communication networks were interfered on the cyberspace and Ukrainian government members' phones were hacked can also be included in this. These cyber incidents by Russia all hampered the ability of the Ukrainian side to mobilize counter forces against the pro-Russian troops and led to the erosion of military superiority of Ukraine.

Russian hacking of Ukrainian grid electricity facilities is an indicator of the interference with Ukrainian sovereignty, since the operationalization scheme includes articles called "provision of infrastructure services" and "management of the state's assets." During the cyber attacks by Russia, the fiber backbone of the UkrTelecom was destructed, which physically and literally cut the Crimean peninsula from the other Ukrainian territories and made it easier for Russia to occupy it in hours.

Lastly, the international relations segment of this sovereignty operationalization scheme can also be said to be impaired in the case of Ukraine, as

the Ukrainian state lost the capacity to enter into international relations for Crimea, as it changed its status as one of its sovereign territories and annexed by another country. Crimea is now lost to Ukraine and though most of the countries do not recognize Crimea as part of Russia, it is now de facto under Russian control. Thus it can be clearly asserted that, with the help of the cyberspace use, the Ukrainian sovereignty on deciding on the international status of the Crimean peninsula is disrupted, with the peninsula lost on ground.

All in all, when these indicators are reviewed again, the Ukrainian sovereignty can be said to be eroded clearly, due to the intense use of cyberspace by the Russian cyber forces backed by Kremlin.

### 5.1.3 Stuxnet

Stuxnet case is another case that exemplifies a situation in which two (actually with the help of another one, three) nation states get involved and through the cyber methods, the sovereignty of one of them is significantly diminished in a specified field (namely, the nuclear one). Besides this, Stuxnet is a case that involves some kind of a secrecy around it, since the active state that prepared Stuxnet does not officially accept responsibility for it, while the state that got severely affected by Stuxnet attack does not officially accept it either, since it does not want to confess its cyber weaknesses, which might cause other states or other rival actors to perpetrate more cyber attacks. Despite the lack of official explanations from either side, Stuxnet is one of the most significant cyber incidents in history, both in terms of the scope of its detailed code design and in terms of the damage it cost for another nation-state's nuclear enrichment program.

Stuxnet is basically a malicious computer worm that was developed together by the US and Israel and it was intended for destructing or at least delaying Iran's nuclear program without being noticed. Although the US and Israel never acknowledged having orchestrated it officially, all the technical reports released by independent sources lead to the two. Stuxnet still continues to confuse technical scientists and political scientists, since it was specifically designed for a specific Iranian nuclear plant (and was designed so professionally) and it was able to escape from that specific nuclear plant and was able to inflict many other computer systems (Langner, 2013). The possibility of a nation-state's involvement in such activity (although the probability of which constitutes more than just a "possibility") has raised concerns regarding the prospects of cyber war that was previously thought to only be feasible in fiction.

Stuxnet was first discovered in June 2010 and is the name given to the cyber weapon which was designed to attack the Natanz nuclear facility in Iran. No state has yet assumed official responsibility for the attack, although all the technical reports made it clear again and again that it was developed by the US and Israel. Neither state has denied the allegations. In his famous 2011 book titled *Confront and Conceal*, David Sanger argues that Stuxnet was developed at NSA headquarters in Maryland and was tested on a model nuclear plant in Israel. The fact that Stuxnet generously employed zero-day exploits which are worth hundreds of thousands of dollars on the exploit markets supports the argument that it was developed with the support of a nation state budget. Indeed, Stuxnet is believed to have cost a few million dollars (Can, 2014a). In addition, comprehensive technical speculation has named Israel's Military Intelligence Unit 8200, known for its advanced Signal

Intelligence (SIGINT) capabilities, as the possible creator of the software, as an aide to the United States (Student Daily News, 2010).

The way Stuxnet operated in the nuclear facility is extremely intelligent and utterly sophisticated. Though the Natanz nuclear site was cut off from the global internet network, as all SCADA systems are when confronted with security concerns, Stuxnet still somehow managed to find a way into the plant, most probably through third-party contractors working with the site. Stuxnet primarily attacked the IR-1 centrifuges that enrich uranium, altering their speed and reducing their usability time without being detected by the control engineers. In this way, Stuxnet is believed to have set back the Iranian enrichment facility by two years despite the fact that no existential harm was inflicted on the plant (Can, 2014a).

It soon became clear, in the code itself as well as from field reports, that Stuxnet had been specifically designed by a nation-state to subvert Siemens systems running centrifuges in Iran's nuclear-enrichment program. The Kaspersky analysts at the time realized that financial gain had not been the objective in creation of the cyber weapon. It was a politically motivated attack. "At that point there was no doubt that this was nation-state sponsored," Schouwenberg asserts. This phenomenon caught most computer-security specialists by surprise. "We're all engineers here; we look at code," says Symantec's O'Murchu. "This was the first real threat we've seen where it had real-world political ramifications. That was something we had to come to terms with" (Kushner, 2013). Kevin Hogan, Senior Director of Security Response at Symantec, noted that 60% of the infected computers (infected by Stuxnet) worldwide were in Iran, suggesting that its industrial plants were the target (Student Daily News, 2010). According to the claims of *the New York Times* from his first months in office onwards, "President Obama secretly ordered increasingly

sophisticated attacks on the computer systems that run Iran's main nuclear enrichment facilities, significantly expanding America's first sustained use of cyberweapons, according to participants in the program" (Sanger, 2012).

It was thus recorded in the history of cyber security that the United States used a cyberweapon for the first time against another country in order to cripple its infrastructure, achieving, with computer code alone, what until then could be accomplished only by bombing a country or sending in agents to plant explosives. The cyber weapon Stuxnet was 50 times as big as the typical computer worm, Carey Nachenberg, a vice president of Symantec, one of the many groups that have dissected the code, said at a symposium at Stanford University (Sanger, 2012). The forensic investigations and reports all showed quite obviously that "the technical expertise and human intelligence sources needed to create and deliver what was described as the 'world's first cyberweapon' pointed to a joint operation by American and Israeli agencies" (Williams, 2012). However, it escaped from Natanz and infected cyber systems in as far as Indonesia, India and ironically, the United States (Pauli, 2013).

The functioning of the Stuxnet cyber weapon was briefly as follows: The uranium enrichment of the nuclear plant was achieved through centrifuges, actually hundreds of them working at the same time. Centrifuges, which can be visualized as cooking pots that revolve around themselves at extremely high speeds so that the uranium inside them could be enriched. Stuxnet was designed to first increase the normal speed of these centrifuges to double or triple the amount of the usual speed, and then decrease it to extremely low speeds, which resulted in the breaking of many centrifuges one by one. More technically-speaking:

> [t]he normal operating speed of the IR-1 centrifuge is 63,000 revolutions per minute (rpm). Stuxnet increased that speed by a good one-third to 84,600 rpm for 15 minutes. The next consecutive run brought all centrifuges in the cascade basically to a stop (120 rpm), only to speed them up again, taking a total of 50 minutes. (Langner, 2013)

The engineers and controllers working in the Natanz nuclear facility were not able to detect the failure of centrifuges because they were wearing protective earplugs while they were working, and secondly, Stuxnet virus showed a pre-recorded screenshot again and again on control screens, rather than the actual real situation of the nuclear enrichment process. According to the experts,

> Stuxnet records the cascade protection system's sensor values for a period of 21 seconds. Then it replays those 21 seconds in a constant loop during the execution of the attack. In the control room, all appears to be normal, both to human operators and any software-implemented alarm routines. (Langner, 2013)

As for the effects of Stuxnet, it is a "low-yield weapon with the overall intention of reducing the lifetime of Iran's centrifuges" and not destructing them totally. This means that by reducing the lifetime of the centrifuges, they broke down one by one, instead of getting destructed in a wholesome way. The reason for this is that a total destruction of the centrifuges would drive too much suspicion of the Iranian side and thus would fail. By working at a slow pace, Stuxnet was able to delay the huge Iranian nuclear program by at least two years (Langner, 2013). Besides delaying the whole program at the Natanz nuclear facility, Stuxnet additionally delayed the start up of Iran's Bushehr Nuclear Power Plant, according to technical reports (Student Daily News, 2010). The reports regarding the damage that Stuxnet inflicted on the Natanz nuclear plan of Iran was well documented looking at the number of centrifuges destructed with no cause at all. Stuxnet reportedly ruined almost one-fifth of Iran's nuclear centrifuges (Kelley, 2013).

The graph in Figure 11 tells a lot about the Iranian nuclear program and Stuxnet's effects on it. The middle of the graph shows a point where the number of centrifuges actively used in the Natanz nuclear facility actually starts to drop abnormally. The Iranian authorities realized this fact that the centrifuges were breaking down one by one for no reason, and in order to ensure a constant enriched uranium output, they produced spare centrifuges and kept them aside, in increasing numbers. The effect was solely because of Stuxnet. While the number of centrifuges in use decreased, the number of centrifuges that are kept in spare constantly increased during this process.

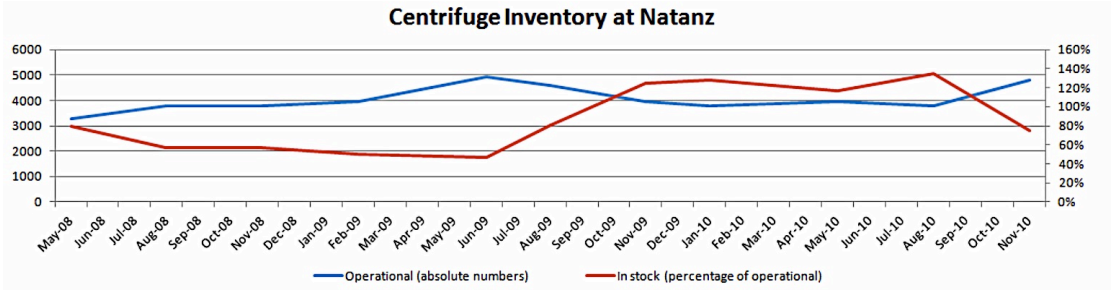


Fig. 11. Centrifuge inventory at Natanz between 2008 and 2010 (Source: Langner, 2013)

In order to truly understand what this Stuxnet-caused delay meant in terms of nuclear plant enrichment process, Langner's (2013) comparison of Iran with Pakistan is truly helpful:

> When comparing the Pakistani and Iranian uranium-enrichment programs, one cannot fail to notice a major performance difference. Pakistan basically managed to go from zero to successful low-enriched uranium production within just two years during shaky economic times, without the latest in digital control technology. The same effort took Iran over 10 years, despite the jump-start from Pakistan's A.Q. Khan network and abundant money from sales of crude oil.

Besides influencing the sovereignty of Iran over its own nuclear program, according to cyber security experts, Stuxnet also helped to send a powerful message regarding the cyber arsenal of the US to other countries, especially Russia and China. As Langner aptly argues, Stuxnet "saved America from embarrassment. If another country — maybe even an adversary — had been first in demonstrating proficiency in the digital domain, it would have been nothing short of another Sputnik moment in U.S. history" (Langner, 2013).

After looking at Stuxnet and its functioning, it is now the time to analyze the case in terms of the nation-state sovereignty. In order to achieve this, we should apply the sovereignty operationalization scheme put forward by Ghani, Lockhart & Carnahan and look and the indicators of this scheme one by one, whether they were affected in any way by Stuxnet cyber weapon and the use of cyberspace by the US and Israel against the interests of Iran. The areas where the Iranian sovereignty are seriously affected are shown with an asterisk sign (*), since they show erosion on the part of the Iranian state. The table, then, in this case, would look like Table 4.

Table 4. Sovereignty Operationalization of Stuxnet Case

| | |
|---|---|
| Legitimate monopoly on the means of violence | * |
| Administrative control | |
| Management of public finances | * |
| Investment in human capital | |
| Delineation of citizenship rights and duties | |
| Provision of infrastructure services | * |
| Formation of the market | |
| Management of the state's assets (including the environment, natural resources, and cultural assets) | * |
| International relations (including entering into international contracts and public barrowing) | |
| Rule of law | |

As can be seen from the data presented in Table 4, the cyber weapon Stuxnet delayed the Iranian nuclear enrichment plans for at least two years, and it deprived Iran from the means and ability to control a plan which it sees fit. Just in the same way that the Ukrainian sovereignty was impaired in the previous case, the Iranian sovereignty eroded, at least in terms of a specific program of its own, to which it attributed hugely political meanings.

Firstly, Stuxnet delayed the nuclear plans of the Iranian government by two to four years, the plan at the Natanz nuclear facility was totally disrupted and the startup of Bushehr Nuclear Power Plant was hindered according to technical reports. Stuxnet, in addition, reportedly ruined almost one-fifth of Iran's nuclear centrifuges. These all impaired the sovereignty of the Iranian state in terms of the articles checked on the table. The monopoly of the Iranian state on the means of violence can be said to be impaired, because the nuclear enrichment plans for the development of possible nuclear weapons were hindered. The nuclear enrichment of the uranium by Iran is clearly for the nuclear weapon and defense purposes. The hindrance of the nuclear enrichment thus means a prevention of the Iranian defense industry program, and also means that Iran lost its sovereignty on the issues such as monopoly on the means of violence, management of public finances and management of the state's assets (on the nuclear issue in this case.)

Secondly, the management of public finances and the provision of infrastructure services were negatively influenced due to Stuxnet, since nuclear enrichment both includes state plans regarding its budget and also it concerns the infrastructure services of Iran, since nuclear enrichment gives (or is thought to give) rise to electricity grid services. Nuclear energy sources of a country are hindered in

this case, which in turn can be said to be an erosion of Iran's sovereignty on provision of infrastructure services issue.

Management of the state's assets article on the sovereignty operationalization scheme is also checked, since Iran's ability to use its nuclear enrichment resources at its will was severely disrupted. Nuclear enrichment is an asset of the Iranian state without any doubt, and under normal circumstances, we would expect it to be the sole sovereign on the nuclear enrichment plans. However, Stuxnet prevented it from achieving full sovereignty.

Bearing in mind all these effects of the Stuxnet cyber incident, we can claim Iran to have lost some part of its sovereignty on the related nuclear issue, as shown on the sovereignty operationalization table through sovereignty indicators.

### 5.1.4 Egyptian Revolution

The role of the Internet is well known in the Arab Spring in general and a field that has been well studied within the scope of political science and sociology in the recent years, as well as communication studies disciplines. This role could actually be analyzed in lengthy details, however, this is not a primary topic of the thesis and Egypt is just a case among other cases, so it will be reviewed rather shortly. The previous cases in the chapter, like the Stuxnet case, were cases that contained a relationship from a state to another state. However, in the Egyptian Revolution case, we will witness a case that included a cyber sovereignty relationship between a nation state and its subjects. The case makes it clear that the Egyptian state's sovereignty was eroded due to the intense use of cyberspace by the citizens over a specific amount of time.

In order to understand the role of cyberspace in the Egyptian revolution, we should look at the history of the event shortly. In the year 2011 and on the morning of 25 January 2011, mass protests erupted in Cairo's Tahrir Square in which Egyptians called for an end to the rule of the then-president Hosni Mubarak. There had been smaller social movements in the past against the same authoritarian rule, but the 2011 revolution surpassed all, in terms of number and effect, due to the additional use of cyberspace.

In various parts of Egypt, but mostly in the Tahrir Square in Cairo, protests occurred. Especially in the Tahrir Square the number of the protestors that gathered was estimated to be up to two million (Alexander, 2011). The protests were mostly peaceful, with protestors holding signs and chanting anti-government slogans. The regime, in the traditional authoritarian way, sent police forces that were heavily armed together with water cannons, which immediately led to further tensions between protestors and the police forces. Mubarak government also implemented curfews to end this unprecedented protest wave. However, due to the use of cyberspace and social media, the idea that the curfew was unrightful spread quickly and the protestors adhered even more to their cause. All the attempts by the government in order to put an end to the protests turned the situation even worse on the part of the government and created a stronger and more decisive divide between the government and those demanding political reform (Alexander, 2011). The protests across Egypt coordinated by a loose coalition of opposition groups - many of which are very largely organized through Facebook - seemed to demonstrate that social media use would heavily contribute to the mobilization of protests. "Certainly, the Egyptian government reacted quickly: blocking social media sites and mobile phone networks before pulling the plug on Egypt's access to the Internet"

(Alexander, 2011) however, these measures did not work. In the words of a first-hand journalist witness of the January 25 protests:

> I was in Tahrir Square on Sunday: everywhere you look there are mobile phones, hand-written placards, messages picked out in stones and plastic tea cups, graffiti, newspapers and leaflets, not to mention al-Jazeera's TV cameras which broadcast hours of live footage from the square everyday. When one channel of communication is blocked, people try another. (Alexander, 2011)

The sentences of a social activist from the anti-government protests sheds light on the role of cyberspace. When asked about the Internet's role in mobilizing the protest he said: "Online organizing is very important because activists have been able to discuss and take decisions without having to organize a meeting which could be broken up by the police" (Alexander, 2011).

The web-use statistics dating back to the protests show that even in poor urban and rural areas the Egyptians' access to Internet was not broken thanks to shared connections. One of the key organizing centers of the protests, for instance, was the Facebook group that was set up to protest Khaled Said's death, and due to its sentimental content, 600,000 people liked the page in a few days (Alexander, 2011). The use of social media got such a high impetus that "according to the Project on Information Technology and Political Islam the number of tweets posted about Egypt – many using #Jan25 in homage – jumped from 2,300 to 230,000 per day the week before Mubarak stepped down on the 11 February" (Shearlaw, 2016) and as a result of this, "Foreign Policy magazine declared the Egyptian revolution the Twitter "news moment" of the year" (Shearlaw, 2016).

One Cairo activist spoke out about just how important social media use was in organizing protests and for people to communicate with one another: "We use Facebook to schedule the protests, Twitter to coordinate and YouTube to tell the

world" (Currie, 2015). After the Mubarak government saw that the main force behind the protests was the social media, it made an attempt to stop the use of social media. All the social media websites were blocked in Egypt from the 28$^{t}$ January 2011 to the 1 February 2011. The authorities also blocked the cell networks which made communication virtually impossible. These measures were not effective as they were thought to be, because most of the organization of the protests had been done prior to the blackout (Currie, 2015). The social media was also used by the Mubarak government to advance their arguments and to calm down the situation throughout Egypt. Text messages praising the rule of Mubarak and his alleged contributions to Egypt were sent to the cell phone users in an attempt to save the regime from crumbling. Only Egyptian news agencies were allowed in the country and the news platforms like Al Jazeera and Al Arabiyya were censored (Currie, 2015). The statistics of the social media usage in Egypt during the revolution period were staggering and are worth looking at:

> 78% of Egypt's Facebook users between the ages of 15 and 29, 87% of Egyptians had a phone, 100%+ Twitter user growth during Q1 of 2011 during the time of the revolution (despite a temporary block out by the government), out of all Arab countries, Egypt had the highest increase in the number of Facebook users in Q1 of 2011, 8.7 million YouTube pages were viewed in Q1 of 2011, most popular Tweets in 2011 in Arab countries were: #Egypt, #Jan25, #Protest along with #Bahrain and #Libya, which were both experiencing their own mass protests. (Chebib, Kassem & Sohail, 2011)

The reason behind the political significance of social media is that it allows people to contribute to a virtual public discourse that would otherwise be impossible for them to have access to (Bossung, 2011). For them, the cyberspace is a platform where there is no police brutality, hierarchies and corrupt representation (Bossung, 2011). The social media is especially meaningful in the Arap context since "[s]ocial media provides real-time information, up-to-date and unmolested, unlike Arab state

television and government propaganda. Freedom of the internet means that people choose their sources, and those reputed as trustworthy rise to the top" (Bossung, 2011).

One study regarding the use of cyberspace freely by the Egyptians is striking in terms of the recently recognized importance of social media. The graph in Figure 12 presents an analysis of the nature of the tweets both during and after the January protests.

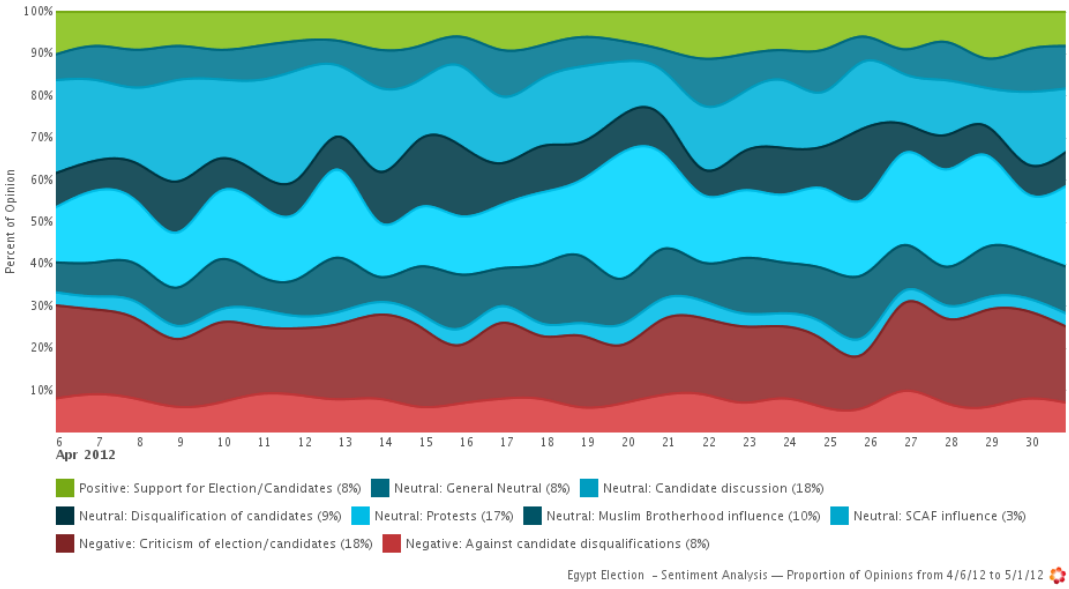


Fig. 12 The graph of the analysis of tweets of the Egyptian revolution (Source: Crimson Hexagon, 2016)

The analysis shows us the Egyptian sentiment on Twitter and, as it can be seen from the data, the public opinion reflected by the public is primarily negative, "with 26% expressing negative sentiment and just 8% expressing optimism about the election and candidates. Of the negative opinions, 18% generally criticize the elections, while 8% express specific opposition to the disqualification of candidates by the election commission" (Crimson Hexagon, 2016). The 17% of the overall

conversation is constituted of the protests generally, and this rose to 30% of conversation on April 20 around the time of the protests in Tahrir Square (Crimson Hexagon, 2016).

Figure 13 shows the examples of the sentiment and intensity of the social media usage during the January 25:

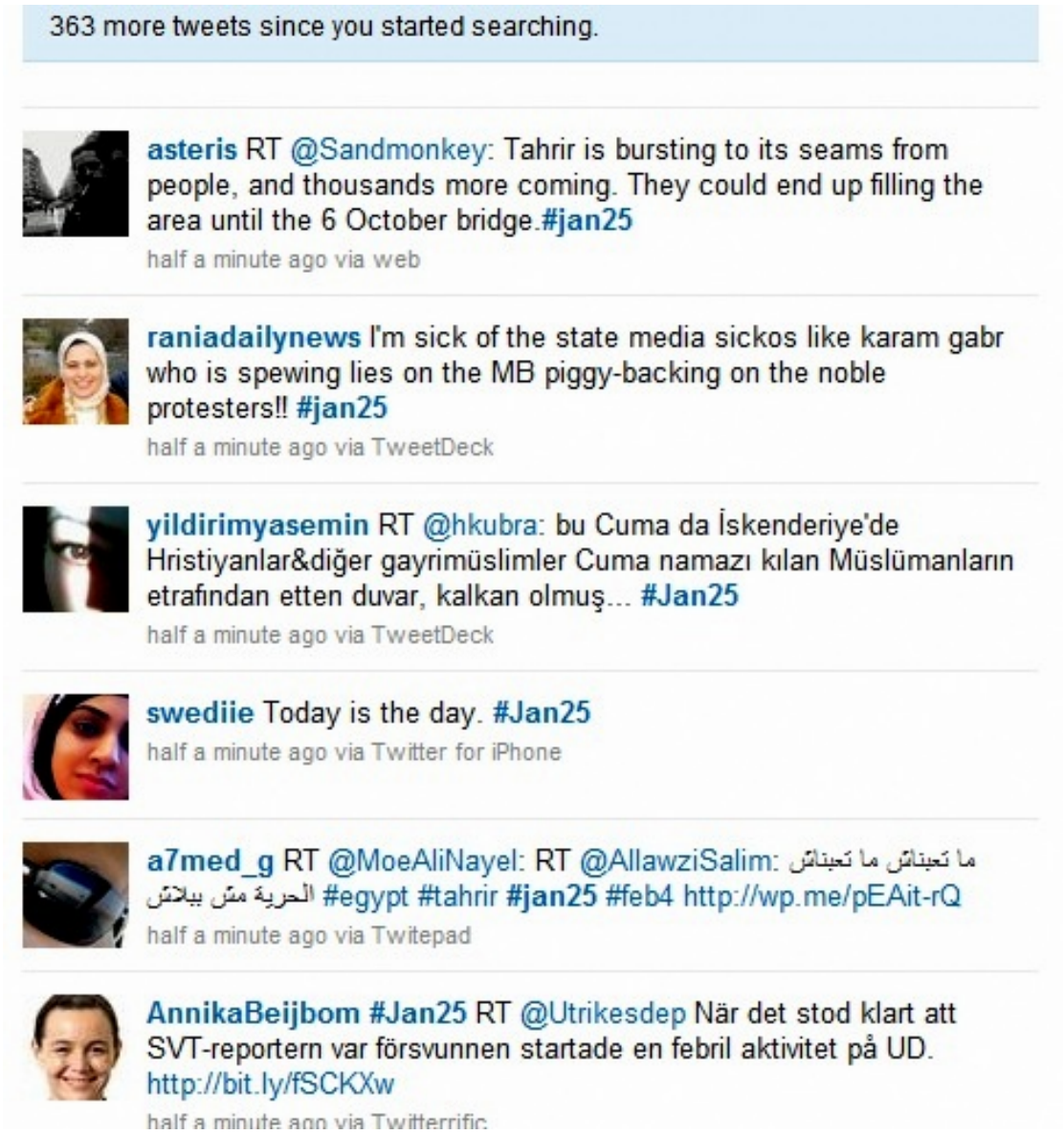


Fig. 13 Tweet examples from January 25 (Source: Twitter)

As can be seen from the example tweets in Figure 13, the messages were sent in multiple languages, while the tweet in Figure 14 shows an example which instantly informs the audience about the cyber practices of the Egyptian government and turns the public attitude against it.


Fig. 14 Tweet example from January 25 (Source: Twitter)

The tweets in Figure 15 and Figure 16 are also indicative of the same phenomenon:


Fig. 15 Tweet examples from January 25 (Source: Twitter)

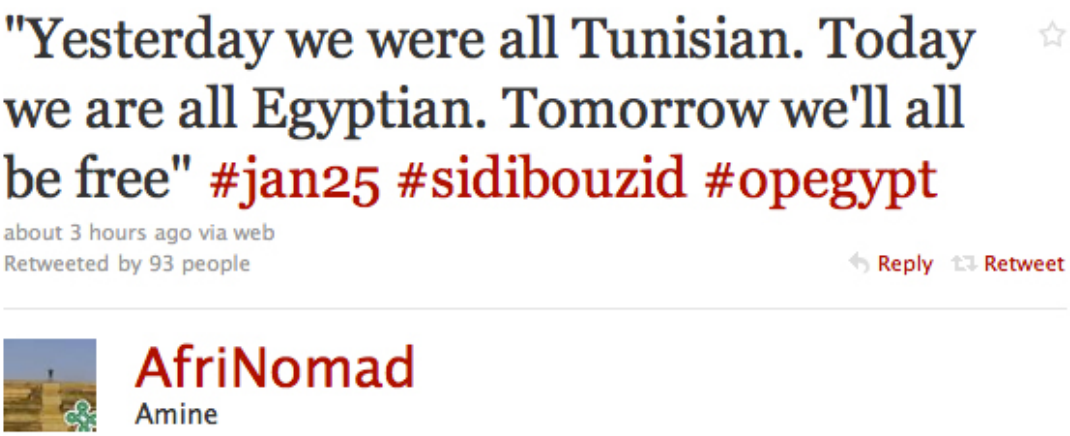


Fig. 16 Tweet example from January 25 (Source: Twitter)

The Twitter was also flooded with tweets that said the looters during the protests were carrying police IDs on them, and this increased the anger against the government even more (Boyd, 2011). The anti-government "narrative" got more consolidated even more in the cyberspace, when the international media organs started to reflect the protests as "uprising" and "chaos" in Egypt. CNN on-screen headlines, during the protests, were "Chaos in Egypt" and "Uprisings in Egypt" (Boyd, 2011).

The protests and cyber activities by the Egyptian masses met with authoritarian preventive measures from the government. The Egyptian government decided to cut all communication systems, including the Internet and mobile phones, however, the interesting point here that, this decision to cut the communication system, "on the night of 27 January was widely perceived to be a watershed moment in the overthrow of the Mubarak government" (New Internationalist, 2016). Since the Egyptian protest sympathizers were not able to watch or follow the events, they took to the streets and joined the massive demonstrations in Tahrir Square instead of sitting in their homes (New Internationalist, 2016). As a result of these processes, the

Mubarak government stepped down on February 12 and a military council that seemingly supported the democratic demands of the Egyptian people came to temporary power, which was soon followed by the democratic elections in the country during which the Muslim Brotherhood party got the majority of the votes.

Now when we have a look at the sovereignty of the Egyptian government and how it got affected as a result of the Egyptian people's active use of cyberspace, using the sovereignty operationalization scheme offered by Ghani, Lockhart & Carnahan, we get the following table. Table 5 uses asterisk signs (*) to indicate the sovereignty measurements points on which Egypt's sovereignty got seriously eroded due to the heavy use of cyberspace by the dissident groups.

Table 5. Sovereignty Operationalization of the Egyptian Revolution Case

| | |
|---|---|
| Legitimate monopoly on the means of violence | |
| Administrative control | * |
| Management of public finances | |
| Investment in human capital | |
| Delineation of citizenship rights and duties | * |
| Provision of infrastructure services | * |
| Formation of the market | |
| Management of the state's assets (including the environment, natural resources, and cultural assets) | |
| International relations (including entering into international contracts and public barrowing) | |
| Rule of law | * |

Now it is time to look at the sovereignty indicators on the sovereignty operationalization scheme to see on which areas the Egyptian state's sovereignty got negatively affected.

Firstly, administrative control capabilities of the Egyptian government suffered a serious blow as a result of the massive protests that it could not actively prevent. The Egyptian state was not able to provide security and order, and an efficient

prevention of the protests mobilized on the cyber space, and this affected the administrative control power of the Egyptian state.

Secondly, the capability to delineate and define citizens' rights and responsibilities, which is an indicator of a state's sovereignty according to the table was also affected. Egypt's ability to control the definitions of loyal citizens' rights and responsibilities also got negatively affected, since these were redefined by the Egyptian people's demands on the fields. Egyptian people themselves redefined what these were, in contradiction to the state's own understandings, and this comprises a sovereignty violation on the part of Egyptian state.

Thirdly, as seen from the table, provision of the infrastructure services is an indicator of the sovereignty of a state. The infrastructure services, like the municipality and police security services, were not delivered for quite some time, as a direct result of the protests again. For extended periods of time, these kinds of services were not delivered to the Egyptian people.

Finally, the rule of law in the country, as understood by the Egyptian government, came to a halt because of the massive protests organized on cyberspace. All in all, we can come to the sound conclusion that the Egyptian state's sovereignty on various issues got negatively affected, as a direct result of cyberspace use by masses.

### 5.1.5 2014 Sony Pictures Entertainment Hack

On November 24, 2014, a hacker group which identified itself by the name "OurMine" (OurMine Team) leaked a release of confidential data from the film studio Sony Pictures Entertainment. The leaked data included sensitive personal information regarding Sony Pictures employees and their families, e-mails between

employees, information about executive salaries at the company, copies of then-unreleased Sony films and some other sensitive information (State of California Department of Justice Office of the Attorney General, 2014). The reason of the hacking was allegedly a film named *The Interview*, a comedy about a plot to assassinate North Korean leader Kim Jong-un. The hacker group OurMine Team demanded this film to be stopped from screening and also threatened with terrorist attacks at cinemas screening the film. The film was stopped from screening, and Sony Pictures Entertainment stepped back in the face of the heavy load of the leaks and the seriousness of the threats. The United States intelligence analyzed the software, techniques and network sources used in the hacking process and came to the conclusion that the attack was sponsored by North Korea, although North Korea denied any connection to hacking and responsibility (Sanger & Perlroth, 2014). It is not yet known how much the duration of the hacking was but technical reports make it clear that it took more than a year. According to the claims of the hackers, more than 10 terabytes of sensitive data was stolen from Sony (Pagliery, 2014). US-CERT, the cyber authority of the US, reported that "the attackers used a Server Message Block (SMB) Worm Tool to conduct attacks against a major entertainment company" (Lennon, 2014) and components of the attack included "a listening implant, backdoor, proxy tool, destructive hard drive tool, and destructive target cleaning tool. The components clearly suggest an intent to gain repeated entry, extract information, and be destructive, as well as remove evidence of the attack" (Lennon, 2014).

When the Sony employees' computers got inoperable as the result of the hacking, the company was made aware of the cyber attack. Sony immediately informed the FBI and private security company FireEye and asked for help to protect

the sensitive employee information, to repair the damaged computer infrastructure and trace the source of the leak (Seal, 2015). The first technical reports regarding a possible North Korean link to the attack was published by Re/code in the later phases and later confirmed by NBC News (Hesseldahl, 2014).

Figure 17 shows the poster of the movie that caused the Sony Entertainment Co. Hacking, *The Interview*.


Fig. 17 The poster of the film that caused Sony Entertainment Co. Hacking, *The Interview*.

North Korean officials had previously directed their official concerns regarding the content of the film (assassination of the North Korean leader) to the United Nations and stated that "to allow the production and distribution of such a film on the assassination of an incumbent head of a sovereign state should be regarded as the most undisguised sponsoring of terrorism as well as an act of war" (Beaumont-Thomas, 2014). The FBI also officially expressed that the infrastructure used in the Sony Entertainment cyber attack was strikingly similar to some other malicious cyber activity that targeted the United States from North Korea (Laughland & Rushe, 2014). After the technical reports linked the hacking incident to North Korea, Samantha Power, the US Ambassador to the United Nations said:

> This is absurd. Yet it is exactly the kind of behavior we have come to expect from a regime that threatened to take 'merciless countermeasures' against the U.S. over a Hollywood comedy, and has no qualms about holding tens of thousands of people in harrowing gulags. (Democracy Now, 2014)

As a result of the hack, Sony (and the US) stepped back and in the first quarter of 2015, Sony Pictures needed to set aside $15 million to deal with ongoing damages from the hack (Frizell, 2015). The Web was inundated with hundreds of news titled like "America lost the cyberwar over Sony" and the comments from the experts were mainly about the sovereignty loss on the side of the United States:

> No one should underestimate the historic importance of the North Korean cyberwar against America and the collapse of American defenses in the Sony Pictures attack. This was a deliberate assault on sovereign American soil against an American company, costing it millions of dollars in direct damages and hundreds of millions in reputational damages while blocking most of its employees from using their internal systems to get routine work done. […] This attack on American interests began on November 24 when there was a massive hacking assault on Sony. After 24 days of government passivity and ineffectiveness, the theaters caved to the threat of terrorist attacks. (Gingrich, 2014)

Even the US President Barack Obama expressed his reservation on the issue as "We cannot have a society in which some dictator some place can start imposing censorship here in the United States because if somebody is able to intimidate folks out of releasing a satirical movie, imagine what they start doing when they see a documentary that they don't like, or news reports that they don't like" (Laughland & Rushe, 2014). The US President, as a response to the cyber attack, issued an Executive Order on 2 January 2015, and this order enacted some additional sanctions against the North Korean government and a North Korean arms dealer, specifically citing the cyber attack and ongoing North Korean policies (The White House Office of the Press Secretary for Immediate Release, 2015). In addition, he also issued a legislative proposal to Congress to update current laws such as the Racketeer Influenced and Corrupt Organizations Act and introduce new ones to allow federal

and national law enforcement officials to respond in a more efficient way to illegal cyber attacks like the Sony hack (Daunt & Szalai, 2015).

When we apply the sovereignty operationalization scheme to this specific hacking incident, we get the Table 6, where the erosion of the US state sovereignty is indicated with the asterisk signs (*).

Table 6. Sovereignty Operationalization Table of the Sony Entertainment Hacking

| | |
|---|---|
| Legitimate monopoly on the means of violence | |
| Administrative control | * |
| Management of public finances | |
| Investment in human capital | |
| Delineation of citizenship rights and duties | |
| Provision of infrastructure services | |
| Formation of the market | |
| Management of the state's assets (including the environment, natural resources, and cultural assets) | * |
| International relations (including entering into international contracts and public barrowing) | * |
| Rule of law | |

The checked rows on the Table 6 show the areas that got affected regarding the sovereignty of the United States. Firstly, the administrative control of the state over the acts of a specific company, namely, Sony Entertainment Co. was annihilated and damaged. It might constitute a precedent for other companies as well, and they might step back in the case of a cyber attack regardless of the decisions of the sovereign state they are subject to.

Management of the state's assets (in this case, the cultural assets) were damaged, since the power of the state over a specific kind of assets was hindered. Lastly, the ability of the US to enter into international contracts was eroded, since it lost the bargaining power in the face of North Korea, as reflected by the words of the ambassador of the US to the UN.

As a result of the Sony Entertainment Co. Hacking, it might be argued that the sovereignty of the US, at least in this case, eroded. Although the hacking was against a private company and the losses belonged to the private sector, the political authority got affected by it, at least on the discourse.

### 5.1.6 RedHack

The case of RedHack is an interesting one in that, it is an attack against the sovereignty of a nation state (Turkey) through cyber attacks by a non-state actor. RedHack is a Turkish hacktivist (i.e. an activist group that tries to achieve its purposes through cyber attacks) group and it identifies itself with the Marxist-socialist ideology (Ocak, 2012). Although founded much earlier, the group came to the forefront of cyber community and gained popularity in 2012 and since the 27 April 2012 cyber attacks against the Turkish Ministry of Justice and the Turkish National Police, the cyber group has been able to increase its number of followers and cyber attacks (Tatar, 2015).

The most abundant information regarding RedHack comes from the interviews they gave to the media. These interviews reveal that the cyber group was founded on 18 May 1997 and the informatics experts that founded the group were from different nationalities in Turkey (Kübra, 2012). The core group consisted of 12 people at first, but it gets outside help on the occasions that it might need outside help (Ocak, 2012). In line with the Marxist-socialist line it claims to be on, RedHack defines itself as the "voice of the oppressed people," with the motto "Hacking for People." The statement by the group regarding its foundation is as follows:

> The logic in our founding the group is, besides predicting the point the informatics will reach, to be beneficial for our suffering oppressed people in this field and to play an effective role against the censuring and hiding policies of the states that peoples face. (Kübra, 2012)

The group's history also reveals that it aimed to protect the IT systems of the groups that it sympathizes with in the beginning, but it seems that it started to orchestrate attacks itself against the groups that have rival ideologies. While in the earlier periods the group implemented DDoS attacks and webpage defacement attacks, in the later periods it turned to more harmful and large-scale attacks. The DDoS attacks and webpage defacement attacks are just temporary attacks in the cyber realm, and do prevent the access to some websites for a short amount of time. The group, bored with this small-scale understanding of activism, turned to more scandalous attacks later (Tatar, 2015).

The instance that helped the cyber group gain popularity was its hacking the website of the Ministry of the Interior. According to the explanations of the group, the action was intended as a protest against the Minister of Interior who, during a visit to an underdeveloped region in Erzurum, encountered a 60-year old citizen expressing his excitement at seeing him, but reacted by asking: "How will I know that you are excited? Tumble or dance so that I understand" (Cumhuriyet, 2012). The group was frustrated because of this and attacked the ministry's website by posting images and notes regarding the issue.

RedHack conducted 57 cyber attacks between January 2012 and June 2014 and all the targets are located in Turkey (mostly public institutions), except for the Israeli Intelligence Agency attack that was carried out together with Anonymous (Peck, 2013). Most of these attacks are conducted as protests in the face of a specific act of the government, particularly the ones against freedom of expression.

The first attack by the group was an intrusion into the systems of the Ankara Security General Directorate on 27 February 2012, and the incident was reported on the national Turkish media. It was also reported that critical content of the Turkish

security center was stolen (Ocak, 2012). The password of the attacked system was set as “123456” which is one of the most common passwords in the world and among the first to be guessed at in password attacks (Ocak, 2012). During the attack, the stolen content included the complaints that ordinary people made to the police departments, which were extremely private and critical. There were also the contact information of the citizens who made the complaints to the police, and the cyber group published all this information online (Tatar, 2015). Later, the password “123456” was used again to penetrate the electronic document management system of the Higher Education Institution, which led to publication of the stolen content on 8 January 2013 (Ntvmsnbc, 2013).

The newspaper coverage in Figure 18 shows the extent of the hacking scandal:


Fig. 18 Extent of the RedHack hacking scandal from a newspaper

In addition, the content of the hacking was also covered by another newspapers as shown in Figure 19.

Hürriyet Eğitim

Hazırlayan: Nuran ÇAKMAKÇI

**ÖSYS başvurusunda son gün**

2 Ocak'ta başlayan 2013-ÖSYS başvuruları bugün sona eriyor. Üniversite adayları mesai bitimine kadar başvuru merkezlerinden, saat 23.59'a kadar ise internet aracılığıyla başvuruda bulunabilirler.

22

15 Ocak 2013 Salı

# Üniversite arazisi AVM oldu

Redhack dün de Ege Üniversitesi'ne ait yolsuzluk belgeleri açıkladı. Belgeden, Cumhuriyet Başsavcılığı'nın, Ege Üniversitesi'ndeki iddialarla ilgili YÖK'ten bilgi istediği anlaşılıyor. Buna göre, üniversitede suç işlemek amacıyla örgüt kurmak, resmi belgede sahtecilik, ihaleye fesat karıştırmak, görevi kötüye kullanmak, görevi ihmal ve edimin ifasına fesat karıştırmak gibi iddialar ileri sürülüyor. Bunlardan biri de Ege Üniversitesi'ne ait arazinin eğitim amaçlı kamulaştırıldığı ancak daha sonra mevzuata aykırı olarak imar planı tadilatı yapılarak ve alışveriş merkezi yapılması için bir inşaat şirketi ile sözleşme yapılması ile ilgili. 1999 yılında yapıldığı belirtilen sözleşmede, üniversiteye ait 2 bin 500 kişilik yurt yapılacak araziye, daha sonra büyük bir alışveriş merkezinin yapılmasının sağlandığı ifade ediliyor. Sözleşme tarihinden beri göreve gelen yöneticilerin bu duruma göz yumduğu belirtilerek, görevlerini kötüye kullandıkları iddia ediliyor. Belgede sözleşme yapan kişilerin isimleri, alışveriş merkezinin ve inşaat şirketinin adı da açıklandı.




# 60 bin belge paniği

YÖK'ün internet sitesine sızan Redhack'in, gizli ibaresi bulunan belgeleri ele geçirmesiyle birçok üniversite bunlardan nasibini aldı. Redhack, twitter aracılığıyla yaklaşık 60 bin belgeyi ele geçirdiğini duyurdu. ODTÜ olaylarını protesto etmek için YÖK'ün internet sitesini hackleyen Kızıl Hackerlar hakkında YÖK suç duyurusunda bulundu. Yaptığı açıklamada, elektronik belge yönetimi sisteminin 8 Ocak'ta siber saldırıya uğradığı ve gizlilik taşıyan bilgi ve belgelerin hukuk dışı yollarla ulaşılarak paylaşıldığını belirtti. Mahkeme YÖK'ün belge yayınlayan sitelere erişimin engellenmesi talebini reddetti. Öğrenci Kolektifleri, Redhack'in YÖK'ün internet sitesini hackleyerek, bazı üniversitelerin ihale ve malzeme alımı ile ilgili iddiaları yayınladığını savunarak, rektörleri istifaya çağırdı. Ulaştırma, Denizcilik ve Haberleşme Bakanı Binali Yıldırım ise yaptığı açıklamada, "YÖK'ün güvenlik sisteminde zafiyet var. Gerekli tedbirler alınacak" dedi. Redhack son olarak Türkiye Bilişim Derneği Başkanı ve Hacettepe Üniversitesi eski Genel Sekreteri Prof. Dr. Turhan Menteş'e ait yolsuzluk belgelerini yayınladı. Kızıl Hackerlar ayrıca twitter üzerinden #BenTemizimDiyebilecekmisin" hastag'i açtı. Redhack'in saldırısını tüm detaylarıyla inceleyip, saldırının kurum belgelerinin elektronik ortama aktarılması sırasında olduğunu belirleyen YÖK, TÜBİTAK ve emniyet ile güçbirliği oluşturma kararı aldı.



Esat Akıncı

## O kadar para kazanmadım

REDHACK'in önceki gün yayınladığı belgelerde Kars Kafkas Üniversitesi rektörlüğüne her ay 30 bin TL ödeyerek profesör ünvanı aldığı iddia edilen Prof. Dr. Esat Akıncı ve Rektör Prof. Dr. Sami Özcan, Hürriyet'e konuştu. 30 Kasım 2011'de Kafkas Üniversitesi'nde yönetim kurulu onayı ile profesörlük kadrosuna atandığını anlatan Prof. Akıncı, şunları söyledi: "Kafkas Üniversitesi'nden iki yıl ücretsiz izin aldım. İstanbul'da bir özel hastanede Kalp ve Damar cerrahisi ünitesini kurmak üzere legal olarak, yani Sağlık Bakanlığı onayı ile kadrolu olarak çalışmaya başladım. Hakkımdaki iddia son derece gülünç ve saçmadır. Böyle bir parayı ne kazandım, ne de sayın rektöre verdim. Burada aldığım ücret ortalama 15 bin TL civarında. İstenmesi halinde makbuz ve banka belgeleri ile kesinlikle kanıtlanabilir. Bu arada her iki haftada bir Kars'a gidiyorum. Orada Kalp ve Damar Cerrahisi Ünitesi'ni kurdum. Kars'ın ilk açık kalp ameliyatını aralık ayında yaptım. Bu mesnetsiz iftira ile ilgili olarak gerekli yasal işlemleri başlatacağım."



Sami Özcan

## Kanıtlasınlar istifa ederim

KAFKAS Üniversitesi Rektörü Prof. Dr. Sami Özcan ise iddiaları yalanlayarak şunları söyledi: "Konuyla ilgili ihbar mektubu bize geldi. Nedense ihbarda bulunan kişi Akıncı'nın hastanede çalıştığına dair fotoğraflar göndermiş ama para aldığıma dair belge sunamamış. Para aldığım, herhangi bir belge ile kanıtlanacak olursa hem rektörlükten, hem de öğretim üyeliği görevimden istifa ederim. Benim kazandığım para da, ailemin mal varlığı da, kardeşlerimin ne iş yaptıkları da bellidir."

Gönül KOCA

## Sakarya Üniversitesi: Usulsüzlük bulunamadı

SAKARYA Üniversitesi (SAÜ) Rektörlüğü, Redhack'in 1,6 milyon TL'lik banka promosyonunun kullanımında usulsüzlük yapıldığı iddiasına yönelik yazılı açıklama yaptı. SAÜ ile özel bir banka arasında 11 Mayıs 2007'de harç protokolü imzalandığı belirtildi. Protokolün ödeme koşullarına göre 1 milyon 627 bin 333 lirayı aşmayacak şekilde alınan demirbaş ve makine teçhizatının banka tarafından kuruma hibe edildiği vurgulandı. Açıklamada, "Şikayetler üzerine konu Sayıştay, İçişleri Bakanlığı, Vakıflar Genel Müdürlüğü ve YÖK denetçileri tarafından incelenmiş olup, herhangi bir usulsüzlük tespit edilmemiştir" denildi.

Fig. 19 The content of the hacking by RedHack cyber group as reflected on the newspapers.

The cyber security weaknesses such as weak passwords were published online by RedHack since "RedHack never hesitates to reveal such weaknesses in its propaganda. The group claims the weaknesses are indicators of the state's clumsiness

and ineptitude at protecting itself" (Milliyet, 2012). In an interview with Radikal newspaper, which it had previously refused to talk to, RedHack stated:

> We in no way have any connection to the PKK nor with any other terrorist organization, direct or indirect. We get our power from the people itself. We are not terrorists. The fact that we are socialists does not mean that we are terrorists. We are supported by people from every religion, every nation. (Radikal, 2013)

Although founded in 1997, the group gained most publicity in the year 2012. Figure 20 shows a Google trends graph and reflects quite clearly how RedHack's popularity increased in 2012 based on the number of searches of the word "RedHack".

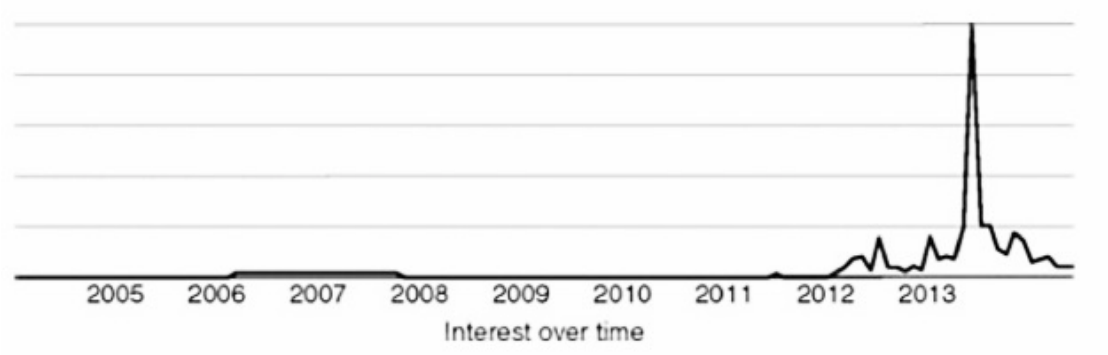


Fig. 20. The Google Trends graph show quite clearly the popularity of the group RedHack based on the number of searches of the word "RedHack" ( Source: Tatar, 2015)

In addition to these hacking activities, RedHack also hacked the website of the Turkish Republic Ministry of Foreign Affairs on 3 July 2012 and published the identities and contact information of US diplomats (Hürriyet Daily News, 2012). It was denounced by the Embassy of the United States in Ankara immediately. The huge cyber attack plans against the websites of the TNP and the Ministry of Justice were partially prevented by the Turkish cyber security officials, however, RedHack

was able to inflict temporary damage. The roles and responsibilities of the state institutions and how they were going to act in the face of a cyber attack were not yet clearly drafted in Turkey during this cyber attack and it raised concerns and speeded the national cyber security processes up.

In order to understand the weakening of sovereignty of the Turkish state, we can refer to the sovereignty operationalization scheme put forward by Ghani, Carnahan and Lockhart. The few areas where the Turkish state might be said to experience sovereignty erosion are shown on Table 7 with asterisk signs (*).

Table 7. Sovereignty Operationalization of the RedHack Case

| | |
|---|---|
| Legitimate monopoly on the means of violence | |
| Administrative control | * |
| Management of public finances | |
| Investment in human capital | |
| Delineation of citizenship rights and duties | |
| Provision of infrastructure services | |
| Formation of the market | |
| Management of the state's assets (including the environment, natural resources, and cultural assets) | * |
| International relations (including entering into international contracts and public barrowing) | |
| Rule of law | * |

The extent of the influences of cyberspace on state sovereignty in this case seems a bit small compared to the other cases, yet it is still significant.

Firstly, the management of the state's assets is eroded, since the websites and other media to reach to its citizens are disrupted due to the hacking and the Turkish state was deprived of such means for quite some time. Although it is on a small scale, the Turkish state's ability to control the information to be delivered to its citizenry is affected due to the hacking incidents, which surely might be followed by

greater incidents such as possibility of posting harmful fake messages on these websites.

Secondly, the rule of law in the country got also affected, since the rule of law as understood by the Turkish state got affected due to the revelations of the secret information to the public. In the same manner, the administrative control of the Turkish state got affected due to the leaks to the public of the administrative information of the Turkish ministries.

All in all, it can be argued that the sovereignty of the Turkish state got influenced and eroded in some ways due to the cyber attacks perpetrated by RedHack. Again, it can be added that the scope of this case is limited. Turkish state's erosion of sovereignty might be argued to be statistically ignorable, however, what makes this case interesting is that it involves a cyber criminal group mobilizing against a nation state.

### 5.2 Sovereignty Strengthened

The two cases that are listed here are the ones in which the sovereignty of a state is immensely strengthened due to its efficient use of cyberspace.

#### 5.2.1 Great Firewall of China

The Chinese President Xi Jinping gave a speech to an international audience at the kickoff of China's second-annual World Internet Conference on 16 December 2015. During the speech, he explained China's vision for what it calls "Internet sovereignty," meaning that others should respect a country's right to regulate online activity as it sees fit. "We should respect the right of individual countries to independently choose their own path of cyber development, model of cyber regulation, and participate in international cyberspace governance on an equal

footing," he said. "No country should pursue cyber hegemony, interfere in other countries' internal affairs or engage in, connive at or support cyber activities that undermine other countries' national security" (Wong, 2015). The President's comments came upon the hotly-debated Chinese Internet policies and were nothing more than the manifestation of Chinese state's insistence on the intense state regulations and controls over the cyberspace.

It needs to be asserted that China, unlike communist North Korea, encourages Internet usage as it tries to build a modern giant economy and the number of Internet users in China surpassed that of the US for the first time in 2008, reaching 233 million by the end of March 2008 (Wiseman, 2008). However, in spite of all the cyber-encouraging efforts by the Chinese state, China's government is the strictest one in terms of tolerating dissent and the variety of opposition views on the Web. China, in order to control its millions of cyberspace users, does not even allow the ordinary social media platforms such as Google, Facebook or Twitter:

> [S]tate-owned media organizations such as the official Xinhua News Agency and China Central Television launched official and verified Facebook and Twitter accounts. On the one hand, Beijing tries to tell 1.3 billion citizens they can't get on Facebook and Twitter inside China. On the other hand, Beijing allows and most likely encourages state media to occupy foreign social media platforms to better tell the China story now that the nation is firmly in the spotlight as the world's number one economy. (Chen et al, 2015)

All the preventive cyber measures mentioned above are further consolidated by a grand cyber project called the Golden Shield Project. "Known extensively as the Great Firewall of China, the Golden Shield Project is a censorship and surveillance project that blocks the data that China sees unfit from other countries" and this project is operated by the Chinese Ministry of Public Security (Jiang, 2008). The centerpiece of the Great Firewall of China effort was the Nation Information Security

Management System, named Project 005 after its starting date in May 2000. The Firewall project won a national prize for science and technology in 2003 and cost more than 60 million USDs, with a huge team of computer engineers working for it (The Economist, 2013). This project is basically a filtering and censorship mechanism, though it is on a much greater scale. Which kind of cyber content will be censored is largely decided politically by State Council Information Office and the Chinese Communist Party's Propaganda Department, with input from other government and public security organs (Harwit & Clark, 2001).

The idea of China's "Internet sovereignty" is a high-profile resurrection of a concept first rolled out in a 2010 white paper called "The Internet in China." As the white paper suggested, the Internet sovereignty of China means "within Chinese territory the Internet is under the jurisdiction of Chinese sovereignty" (People's Daily Online, 2010). According to this provision, all the persons and organizations operating within Chinese territory are expected to follow China's Internet laws and regulations and accept China's absolute sovereignty on the cyberspace (Tiezzi, 2015).

The Chinese censorship and filtering efforts take place on multiple layers of the cyberspace. The Chinese state interferes with the content of the web (on the "information layer" of the cyberspace, according to the cyberspace model offered by Clark,) the Chinese citizens using the cyberspace ("the human layer"), together with the physical devices used to monitor the Internet usage ("the physical layer").

The first layer of the Great Chinese Firewall efforts takes place on the router level, which is part of the physical cyberspace level. According to the 2005 technical analysis of Chinese Internet filtering conducted by the Open Net Initiative, "IAP administrators have entered thousands of URLs (Internet website addresses) and

keywords into the Internet routers that enable data to flow back and forth between ISPs in China and Internet servers around the world" (OpenNet Initiative, 2005; China Internet Network Information Center, 2006). Data flows between the Chinese users and IAP is also controlled, by putting the forbidden keywords and URLs into Internet routers at the ISP level (OpenNet Initiative, 2005; China Internet Network Information Center, 2006).

The illustration in Figure 21 shows the Chinese filtering and censorship practices on the physical layer of cyberspace.

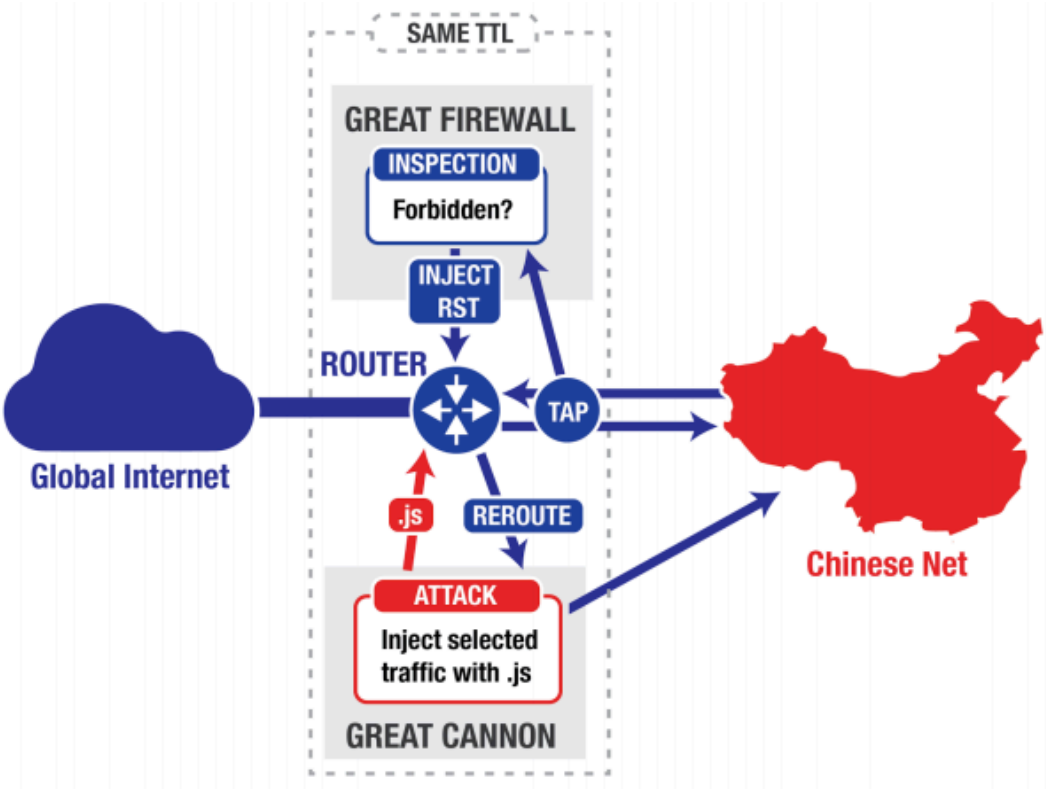


Fig. 21 The Great Firewall of China illustration

Chinese censorship and filtering efforts continue on the "content layer" of the cyberspace as well. The router-level censorship that is reviewed in the previous paragraph is "reinforced by software programs deployed at the backbone and ISP level which conduct additional "filtering" of political content" (OpenNet Initiative,

2005; China Internet Network Information Center, 2006). Such filtering programs that China uses on a grand scale are used normally globally by households, companies, and organizations for all kinds of purposes: they enable employers to block employees from surfing pornography or gambling online from the office, and enable schools to prevent young students from accessing age-inappropriate content (OpenNet Initiative, 2005; China Internet Network Information Center, 2006). The world's leading search engine, Google, along with its many of its helpful utilities like Gmail, Google Maps and Google Drive, are blocked. Similarly, Duckduckgo, a search engine that does not track your online activity, is blocked. Even when you use a search engine that has been approved by the Chinese authorities, there are limitations and censorships on quite many terms and keywords. For instance, spiritually-related topics like Falun Gong and topics related to controversial political events such as Tiananmen Square are not allowed (Mesoznik, 2015). Some terms that would normally be harmless like 'jiang', which means river, are banned due to their association. In the case of jiang, this is a common surname that happens to be tied to the rumors about the death of Jiang Zemin, former General Secretary of the Communist Party of China (Mesoznik, 2015). “Along with specific terms, international new sources, like BBC.com, a number of file sharing sites, like Dropbox, and porn sites are also blocked completely,” and all the social media websites including Facebook, Twitter, Whatsapp, YouTube and Instagram and the like are totally banned (Mesoznik, 2015).

The interesting part regarding the Chinese censorship of all these bans on popular websites is that all these blocked websites have Chinese counterparts. For instance, a website called Baidu is maintained instead of the search engine Google. Twitter is blocked in the country and thus Weibo is used for the same purpose. For

social media purposes and staying in touch with friends and family members, the Chinese population is encouraged to use other equivalent platforms. In this way, the Chinese government is able to maintain a cyberspace that is free of foreign influences and that does not concern about global freedom of speech and information sharing principles. Additionally, these Chinese-origin websites are easier to control as they are closed to the global access (Mesoznik, 2015).

The website usage statistics of the Chinese population can be seen on the graph shown in Figure 22.

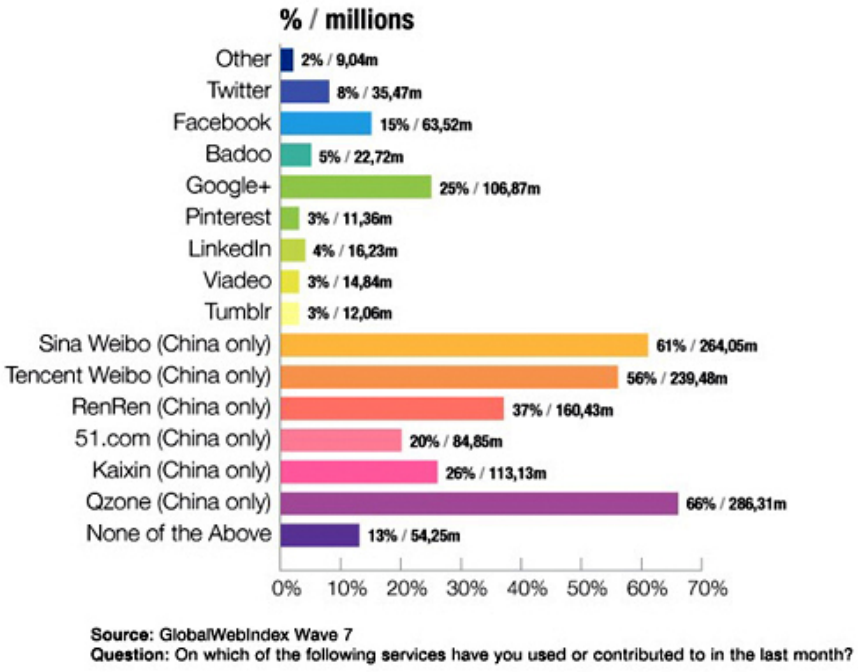


Fig. 22 Chinese usage of cyberspace both in percentages and actual numbers (Source: GlobalWebIndex, 2015)

As can be seen from the graph, Chinese cyberspace users find a way to reach the blocked global websites such as Twitter, Facebook, Google services etc. through various mechanisms but as a percentage, they are really low. The Chinese equivalent services that are used instead of these global websites are extremely popular, on the

other hand and millions of Chinese users are quite active on these government-approved websites. As New York Times makes it clear, "[m]any Chinese Internet users know they are not free online, but they accept this. Online games and myriad social media platforms keep everyone busy. We can make restaurant reservations and shop all we want. Only a small number of people sense what they are lacking" (Xuecun, 2015). Chinese citizens can bypass the government cyber wall by VPNs etc., but it is so rare that shockingly few people do this. According to researchers at the Berkman Center for Internet and Society at Harvard University, "only about 1 to 3% of Chinese Internet users regularly jump the Firewall to browse the open Internet" (Griffiths, 2015). The Chinese Firewall operation is so huge and significant that "one indication of the sheer scale of the operation was given this year by the Chinese state media, which reported that more than two million censors are employed around the country, backed up by an incredibly sophisticated technological platform capable of analyzing web traffic and blocking tools designed to subvert it" (Griffiths, 2015).

In addition to these "content layer" and "physical layer" cyberspace operations, Chinese efforts also continue on the "human layer" of the cyberspace, by trying to control the cyberspace users and by employing humans to monitor and instantly interfere with what is going on in the Chinese cyberspace. For instance, the Guangzhou Municipal Public Security Network Monitoring Division in July of 2006:

> Each Web site shall place a police alert in a visible location on the lower portion of its homepage, and cartoon police alert icons on the homepages of its blogging, discussion forum, and social and other networking pages, which shall lead directly to the designated Web sites of the public security authorities. (Qiang, 2008)

It also added that "[t]he managers of blogging, discussion forum, and social and other networking columns and Web sites must join a QQ chat group set up by

the public security authorities, in order to be contacted during the course of their daily work" (Qiang, 2008).

Thus, to summarize, the Great Firewall of China is composed of following methods combined.

Firstly, "creating bottlenecks", the Chinese government controls the Internet traffic to China by channeling it "through three computer centers — near Beijing, Shanghai and the southern city of Guangzhou" (Wiseman, 2008). By building these chokepoints, "Chinese authorities can easily do something that would be harder in most developed countries: physically monitor all traffic into or out of the country" (Wiseman, 2008).

In addition to this, secondly, the Chinese government "checks the Internet traffic for subversive material" (Wiseman, 2008). In order to achieve this, "the Chinese install "packet sniffers" and special routers to inspect data as they cruise past the chokepoints. If the detectors spot a Chinese Internet user trying to visit a suspect website — say, one run by Falun Gong — they can block the connection" (Wiseman, 2008).

Thirdly, the Chinese government "demands self-censorhip." The Chinese authorities "hold commercial websites responsible for what appears on them. In Beijing — where Internet controls are strictest — authorities issue orders to website managers through cellphone text messages and demand that they comply within 30 minutes, according to a report last fall by Reporters Without Borders" (Wiseman, 2008). The examples of this is that, when the Internet platform Sina.com changed that headline of a state media report on the well-being of the Chinese economy, the Chinese government accused it of "inciting violence" and denied it with access to

interviews with state officials for one month. The website NetEase was forced to lay off two web editors when they published "a 2006 poll showing that 64% of 10,000 participants would not want to be reborn as Chinese" (Wiseman, 2008).

Fourthly, the Chinese cyber authorities issue immense cyber propaganda and "order websites to reprint official propaganda such as a report encouraging Internet users to abide by online etiquette" (Wiseman, 2008). As a fifth method, the Chinese government get outside help when they feel unable to control cyber activities. For instance, the US cyber firms such as Cisco Systems, supply the original routers that Chinese authorities use to monitor the Internet traffic (Wiseman, 2008).

When we try to measure the results of the Chinese cyber practices, we should use the sovereignty operationalization schedule put forward by Ghani, Lockhart & Carnahan. Table 8 shows the areas where the Chinese state's sovereignty got seriously strengthened, using a plus sign to indicate them.

Table 8. Sovereignty Operationalization Table of Great Firewall of China Case

| | |
|---|---|
| Legitimate monopoly on the means of violence | + |
| Administrative control | + |
| Management of public finances | |
| Investment in human capital | |
| Delineation of citizenship rights and duties | + |
| Provision of infrastructure services | |
| Formation of the market | |
| Management of the state's assets (including the environment, natural resources, and cultural assets) | + |
| International relations (including entering into international contracts and public barrowing) | |
| Rule of law | + |

Now it is time to look at the list one by one. The authoritarian Chinese cyber practices have surely influences on enhancing the Chinese grip on the monopoly over

the means of violence, together with the administrative control, as it can be seen from the reviews of these practices above.

Firstly, the cyberspace practices of the Chinese state increases its sovereignty because these practices increase its monopoly on the means of violence. This mechanism works as follows: China does not let any power center other than itself to be formed in the first place. No power group or center can organize against the Chinese state and thus any opposition that might include violence is already prevented from the beginning due to the heavy filtering and monitoring mechanisms of the Chinese state.

Secondly, in a similar way, the administrative control of the Chinese state is also increased. This works as Chinese state's total monitoring of all the activities going on in China's territories and the state's ability to check and monitor the administrative needs and responsibilities of citizens and institutions in the country.

The Chinese state also uses cyberspace to create and develop a concept called "nettizen," the citizens that use cyberspace for patriotic motives, and authorities employ cyberspace to put forward ideal citizen definitions and practices, which ultimately reminds us about the "delineation of citizenship rights and duties" indicator of sovereignty.

Cyberspace can be said to strengthen the management of Chinese state's assets since it helps it organize the cultural assets of the country and authoritarian values thereof. Finally, the rule of law, namely, the rule that the Chinese state sees as the rule of law, is undoubtedly strengthened due to the use and control of cyberspace by the Chinese authorities.

All in all, the cyberspace is a factor that strengthens the sovereignty of China, according to the indicators seen above.

### 5.2.2 NSA Cyber Practices

Edward Snowden, a former National Security Agency contractor, copied and leaked classified information from the NSA in 2013, which disclosed to the public numerous global cyber surveillance programs of the United States government. These cyber programs were mostly run by the National Security Agency in cooperation with some American telecommunication companies and European governments.

Snowden flew to Moscow and he was granted asylum by Russian government, among US charges against him of treason and theft of government property. Though Snowden is still a disputed figure, it is definitely correct that he is one of the most significant figures in the history of cyberspace studies because of his leaks of huge NSA surveillance programs.

The documents revealed to the public by Edward Snowden created shock waves regarding the cyber practices of the National Security Agency. The US was previously thought to be a country which upheld the freedom of speech and the privacy of its citizens both on the cyberspace and on real ground; however, the Snowden documents totally changed this. The NSA practices can be roughly summarized as ten, each scandalous in its own way.

Firstly, it was revealed that Verizon, and together with it, most of the American telephone companies operating in the US were providing private customer information to the National Security Agency. All of the phone records of the customers were shared with the NSA authorities (Franceschi-Bicchierai, 2014). This

revelation is still controversial and still hotly debated though the US President Barack Obama ordered a reform to this practice and it is not yet officially known whether any changes were made to the program.

The second cyber practice of the NSA, an even more scandalous one, is the cyber program known as PRISM. According to the technical reports, PRISM is "the NSA's program to directly access the servers of the US technology giants like Google, Facebook, Microsoft and Apple, among others" (Franceschi-Bicchierai, 2014). Although the NSA does not have direct access to the servers of these companies, it can request user's data from these companies any time and they are required to share the requested information (Franceschi-Bicchierai, 2014). These companies firstly denied the allegations, and later on, they accepted that NSA requires them to share private data with the authority and asked to be more transparent regarding the NSA practices. The third cyber practice revealed by the Snowden leaks is that Britain's intelligence office, GCHQ, has been tapping fiber optic cables all over the world to interfere in the global Internet flow (Franceschi-Bicchierai, 2014). GCHQ is the UK equivalent of the CIA and NSA combined, and has extremely close ties with the NSA in terms of controversial cyber practices. The collaboration program by the GCHQ and NSA is called "Tempora" and contains terabytes of shared information between two intelligence authorities regarding private user information. According to the news of a German newspaper on the Tempora program (Franceschi-Bicchierai, 2014), numerous giant telecommunications companies such as Verizon Business, British Telecommunications, Vodafone Cable, Global Crossing, Level 3, Viatel and Interoute share their users' data with the authorities.

Fourthly, it came as a blow that NSA conducted many activities to spy on numerous world leaders and foreign governments (Franceschi-Bicchierai, 2014). According to the German news magazine *Der Spiegel*, the NSA has targeted at least 122 world leaders including the German Chancellor Angela Merkel, Brazil's former President Dilma Roussef and the French Foreign Ministry (Franceschi-Bicchierai, 2014).

As a fifth revelation, the Snowden documents revealed that NSA uses a program to monitor all the cyberspace users and it is called XKeyscore. XKeyscore is a search tool that can be used to search "nearly everything a user does on the Internet" (Franceschi-Bicchierai, 2014) by data interception. The XKeyscore search system includes into its search mechanism all the private acts of the cyberspace users and is described as the widest-reaching system to search through Internet data (Franceschi-Bicchierai, 2014).

As a sixth NSA surveillance practice, NSA tries to crack encryption and thus prevent privacy. Encryption is a system that locks and protects the communication between two parties and renders this communication to be unreadable to all third parties, such as hackers or surveillance authorities. The NSA has thus developed a series of techniques and tricks to bypass the web encryption technologies used by all other cyber actors (Franceschi-Bicchierai, 2014). Christopher Soghoian, principal technologist at the American Civil Liberties Union (ACLU) said regarding this:

> Even as the NSA demands more powers to invade our privacy in the name of cybersecurity, it is making the Internet less secure and exposing us to criminal hacking, foreign espionage, and unlawful surveillance. The NSA's efforts to secretly defeat encryption are recklessly shortsighted and will further erode not only the United States' reputation as a global champion of civil liberties and privacy but the economic competitiveness of its largest companies. (Franceschi-Bicchierai, 2014)

Seventh, NSA employs highly professional hacking teams and hacking techniques. This elite team of hackers employed by the NSA is codenamed as "Tailored Access Operations" and they hack the computers worldwide by creating malwares and other illegal surveillance operations. When NSA cannot find detailed intelligence or it needs more detailed information about a target, the hackers come into the picture (Franceschi-Bicchierai, 2014).

As an eighth cyber activity, revealed by the Snowden leaks, the National Security Agency also cracks Google and Yahoo data centers, without their knowledge (Franceschi-Bicchierai, 2014). This revelation caused an uproar on the side of the tech companies. Ninthly, National Security Agency collects text messages under a program called Dishfire. Under this program, at least 200 million text messages are collected everyday.

The image in Figure 23 shows the content of the text messages collected by the NSA:

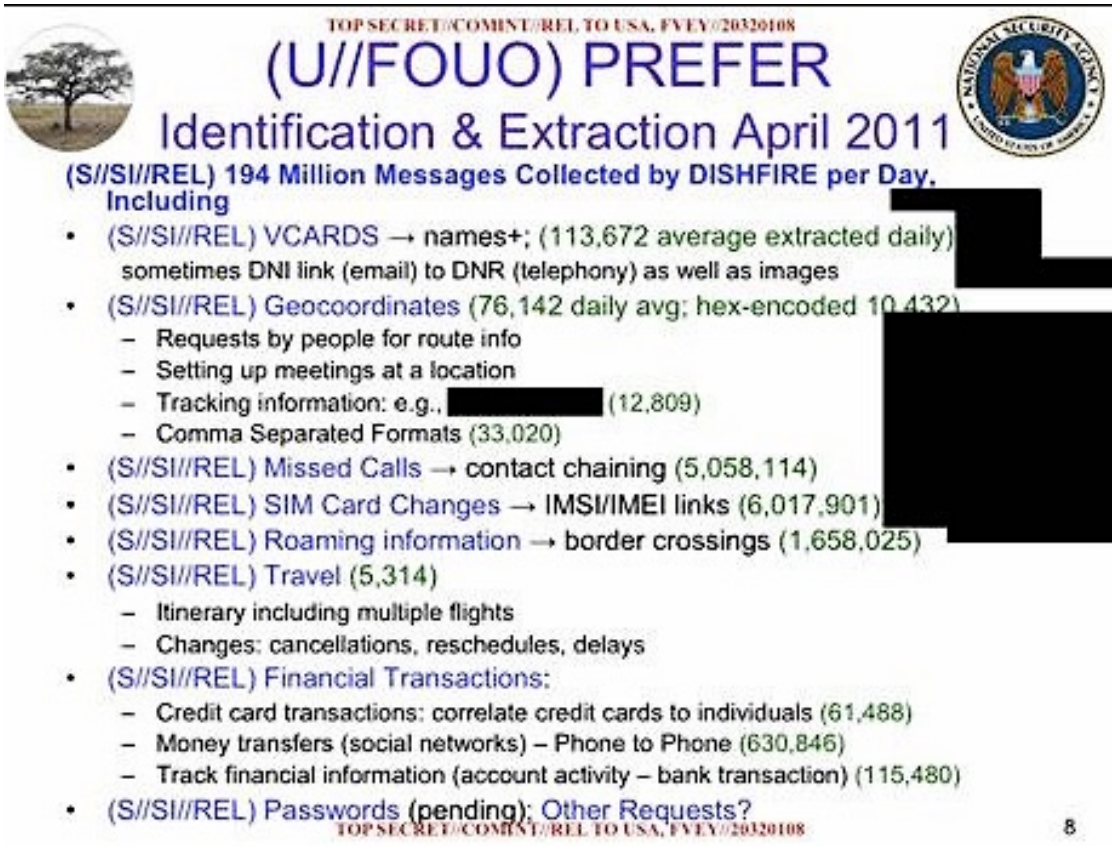


Fig. 23 The content of the text messages collected by the National Security Agency (Source: Franceschi-Bicchierai, 2014)

As the tenth and last NSA cyber practice, it was revealed that NSA intercepts the entire phone calls made in two countries, the Bahamas and Afghanistan. This program is called MYSTIC. The phone calls in these two countries are collected in a whole way. In addition, NSA collects the metadata of the phone calls in Mexico, Kenya and the Philippines (Franceschi-Bicchierai, 2014).

The revelations of the Snowden case revealed one cyber weapon developed by the NSA, as well. Named as "MonsterMind", this cyber weapon is

> autonomous cyberwarfare software platform that can watch international connections to identify and “kill” malicious cyber attacks before they hit American infrastructure — essentially a “cyber missile defense” system tailored to provide protection against the global storm of cyber-attacks. (Templeton, 2014)

One feature of this cyber weapon is that it has the ability to strike back the first attacker. According to the technical and political experts' reports, MonsterMind has the potential to deteriorate international relations if it is used for evil purposes. MonsterMind, besides this, necessitates a massive amount of metadata, which means that a huge collection of the sensitive information is needed for it to work out.

Now, after having a look at the National Security Agency's cyber practices, we can see in how many areas these cyber practices increased the sovereignty of the United States, using the sovereignty operationalization scheme put forward by Ghani, Lockhart & Carnahan. The checked rows on Table 9 show the affected sovereignty indicators, and, since it is argued that sovereignty is increased and strengthened, plus signs (+) are used on the table.

Table 9. Sovereignty Operationalization Table of NSA Cyber Practices

| | |
|---|---|
| Legitimate monopoly on the means of violence | |
| Administrative control | + |
| Management of public finances | |
| Investment in human capital | |
| Delineation of citizenship rights and duties | + |
| Provision of infrastructure services | |
| Formation of the market | |
| Management of the state's assets (including the environment, natural resources, and cultural assets) | |
| International relations (including entering into international contracts and public barrowing) | + |
| Rule of law | + |

Firstly, the administrative control of the United States over its citizens increased due to the extensive use of cyber surveillance mechanisms specified above in name. The fact that the US government obtains the entire private phone calls through getting the sensitive information from the communication companies like Verizon clearly increases the internal sovereignty of the state. In addition, the US

government, as stated above as well, has the ability to intercept into the servers of the companies such as Google and other social media servers,which also serves this purpose.

Its power regarding the defining of citizenship rights and duties has also increased since the cyber surveillance tracked and documented the citizens' information in detail and helped the US come up with additional changes to them. Constantly having the citizens' information under its hand is possible through the NSA's cyber surveillance processes.

NSA cyber surveillance on foreign leaders enables the US to enter into international relations with these foreign countries with even greater say and even more sovereign decisions. The information regarding the potential actions of the states around the world surely serves the US government to take more effective measures and act accordingly, which increases it sovereignty externally in the international arena.

Lastly, the rule of law is strengthened in the country through the disputed cyber surveillance mechanisms. Although these mechanisms are disputed in terms of human rights, the US government uses these cyber surveillance practices to monitor and control possible terrorist activities. In this respect, it can be said that the rule of law in the country (as understood by the US government) is sustained through cyber surveillance practices.

Through the cyber surveillance practices of the NSA, as revealed by the Edward Snowden leaks, the sovereignty of the US can be rightfully claimed to have strengthened.

5.3 Conclusion

Now that we have looked at all the cases that this thesis intends to have a look, a table that summarizes all the cases and their content will be quite informative (Table 10).

Table 10. Summary of the Details of All the Cases in the Thesis

| | Bitcoin | 2014 Russian Dominance of Ukrainian Cyberspace | Stuxnet | Egyptian Revolution | 2014 Sony Pic. Hacking | RedHack Case | Great Firewall of China | NSA Cyber Practices |
|---|---|---|---|---|---|---|---|---|
| The country in the case | Global | Ukraine | Iran | Egypt | USA | Turkey | China | USA |
| The direction of the cyber incident (from-to) | Non-state to State | State to State | State to State | Non-state to State | State to Non-state & State | Non-state to State | State to Non-state | State to State & Non-state |
| Monopoly on the means of violence | - | - | - | | | | + | |
| Administrative control | - | - | | - | - | - | + | + |
| Management of public finances | - | | - | | | | | |
| Investment in human capital | | | | | | | | |
| Delineation of citizens rights & duties | | | | - | | | + | + |
| Provision of infrastructure | | - | - | - | | | | |
| Formation of the market | - | | | | | | | |
| Management of the state assets | - | - | - | | - | - | + | |
| International relations | | - | | | - | | | + |
| Rule of law | - | | | - | | - | + | + |
| Overall Effect of Cyberspace | - | - | - | - | - | - | + | + |

The aggregate table (Table 10) quite succinctly summarizes the findings and arguments of the cases of this thesis. As it can be seen from the details of the table, some of the cases involve a cyber initiative stemming from a nation state, towards the sovereignty of another state, while some of the cases stem from a non-state actor and target a specific state. Some of the cases, on the other hand, have some implications both for specific states and a non-state actor, such as the Sony Entertainment Co. Hacking by North Korea, which both affected the sovereignty of the US as a state and had massive material outcomes for the company itself. Minus signs (-) on the table indicate the areas where state sovereignty got negatively affected and eroded, and the plus signs (+) indicate the ones that state sovereignty is strengthened due to cyberspace.

We have looked at all the cases that support the main arguments of the thesis. However, it is necessary to go on with a small and vital part in this chapter. The part below constitutes of a short guideline for those who will conduct further research and lists down cyberspace factors that hold significance for the sovereignty of nation states. Some of the entries below are a "characteristic" of the cyberspace, while some others are technical software or development, but their common aspect is that they are all factors that might somehow have importance for the sovereignty of nation states, whether strengthening or eroding. For instance, the first feature of the Internet specified below is "the global nature of Internet" and it further explains that the globalness of the Internet creates some complex consequences for the sovereignty practices of the states, mostly in eroding ways. VPN services, for instance, is not a "characteristic" of the Internet, but it is rather a technical service that cyber users employ to bypass the Internet censorship restrictions and might thus have negative effects on the cyber sovereignty practices of states, if they have any.

The global nature of the Internet is self-evident and it requires little knowledge to understand that "globalness" of the web is one of the central features of the Internet. The cyberspace boosts itself mostly on this ability to be "the" platform that is able to connect so diverse and large numbers of users all around the world. Indeed what made the Internet "the Internet" was this very feature, namely, rather than being a local network, within the limits of an institution, a region, or a nation-state, it is a global network that connects networks, which renders cyberspace essentially global and borderless.

As the previous part on the structure of the cyberspace indicated, the Internet started from humble beginnings and it rapidly globalized. Currently, there are more than 2.5 billion Internet users, and the amount is expected to rise to 3.6 billion globally by 2017. The birthplace of the Internet, the US, surely has one of the highest rates of Internet usage in the world, however, over 40% of global Internet users are now based in Asia Pacific. The initials days of the Internet saw only a few primitive websites, and the number of websites today are well over 634 million worldwide, and these websites are in every language imaginable, possible to be reached from everywhere in the world. Even the basic definition of the Internet emphasizes this global characteristic: a global system of interconnected computer networks that use the standard Internet protocol suite (TCP/IP) to link several billion devices worldwide. Although it is true that the physical infrastructure that enables the cyberspace to exist is located within the borders of the nation states, the cyberspace itself is not, since the Internet is basically the name of the connectedness, rather than the connected parts.

As a whole, the Internet consists of many independent networks and is sustained by different people, businesses and regulations, and thus is has been

"designed to be redundant, which means even if one portion of the network goes down users should still be able to get to their destination in most cases" (Post, 2009). For instance, Asia experienced earthquakes, which in turn damaged underwater fiber cables. Despite the fact that the region had some minor problems, the Internet network traffic around the globe and in the region did not entirely shut down in terms of connectivity.

Embedded in the very nature of the Internet, what makes it possible for the Net to be so globally ever-connected might be defined as one of its main communication logic: "packet routing." Packet routing refers to the basic task of sending packets of data (datagrams) from source to destination by forwarding them to the next network router closer to the final destination. At the heart of this routing mechanism lies a logic that different devices with "Internet Protocol addresses," or shortly "IP addresses" are reachable from other devices, since the queries from a device are routed through the network to the destination without any interference or hindrance. This routing flows through principal data routes between large, interconnected networks and core routers on the Internet, which constitutes the Internet backbone. These data routes are hosted and maintained by multiple kinds of parties such as commercial, governmental, academic network centers, Internet exchange points and network access points, which makes it possible for Internet traffic to occur between the boundaries of countries and continents.

This global nature of the Internet alters the way the nation-state territoriality and the accompanying sovereignty practices. As Baase rightly puts it, "the Net radically subverts a system of rule making based on borders between physical spaces, at least with respect to the claim that cyberspace should naturally be governed by territorially defined rules" (Johnson & Post, 1996). Even before delving

into the technical methods of how the state sovereignty is undermined or magnified by these methods, it can be said that the very nature of the Internet as a global network is a major factor that contributes to its being a platform that has the essential potential to challenge state sovereignty. As one of the main features of the modern nation-state system, states have the sovereignty to act within their borders and some other special spaces, however, a space such as the cyber one, with its global nature that does not dwell within physical borders, constitutes a challenge for the apparent reason.

Secondly, though the Internet had its roots at a governmental project outsourced to the private sector, in its later stages it was maintained and regulated by the private sector, which contributed to its being relatively away from governmental regulations and practices. The cyberspace is not totally a private sector platform, surely it is subject to government regulations and interferences, however, a counterfactual will clarify the role of the private sector in the cyberspace: If the cyberspace was purely and solely at the hands of nation states, it would be a place where individual and civic freedoms would not be such fostered.

Thirdly, encryption has some implications for the sovereignty of nation states. Encryption is the process of encoding messages or information in such a way that only authorized parties can read it. Encryption does not by itself prevent interception, but denies the message content to the interceptor. The most significant phenomenon in cyberspace that prevents state inspection, encryption of the communication so that only two authorized parties can reach the information. This might have some implication for eroding the sovereignty of nation states, since they can no longer intercept with the encrypted communication.

Fourthly, as specified in one of the cases above in the cases chapter, social media has double effects on the sovereignty of nation-states. The exceedingly popular use of social media websites has a striking impact to enable millions of citizens to exist in the cyberspace, and question the nation-state practices in an incredible speed and number. Although nation states themselves use social media for political propaganda and awareness-raising, it always lags far behind the collective use of individuals, if at all. The role of social media has been extensively studied especially in the aftermath of the Arab Spring, based on the high usage of social media during the street protests.

As a fifth cyber feature that might have severe effects of the sovereignty of nation states, we can mention the VPN systems. A virtual private network (VPN) extends a private network across a public network, such as the Internet and it enables a computer or Wi-Fi-enabled device to send and receive data across shared or public networks as if it was directly connected to the private network, while benefiting from the functionality, security and management policies of the private network. A VPN is created by establishing a virtual point-to-point connection through the use of dedicated connections, virtual tunneling protocols, or traffic encryptions.

Similar to the VPNs, Onion Routers might also be mentioned in the same vein. Onion routers such as the TOR browser, etc., use a method to roulette the IP addresses of the cyber users, allowing for an effective way to provide anonymity for the users. Onion routing (TOR) is a technique for anonymous communication over a computer network. Messages are repeatedly encrypted and then sent through several network nodes called onion routers. Like someone peeling an onion, each onion router removes a layer of encryption to uncover routing instructions, and sends the message to the next router where this is repeated. TOR (previously an acronym for

The Onion Router) is free software for enabling online anonymity and resisting censorship (Oppliger, 2014, p. 94). It is designed to make it possible for users to surf the Internet anonymously, so their activities and location cannot be discovered by government agencies, corporations, or anyone else. The illustration in Figure 24 shows the functioning of the TOR network. As the diagram in the figure illustrates, the client obtains a list of the available TOR relays from a directory service (1), establishes a circuit using multiple TOR nodes (2), and then starts forwarding its traffic through the newly created circuit (3) (Khandelwal, 2014).

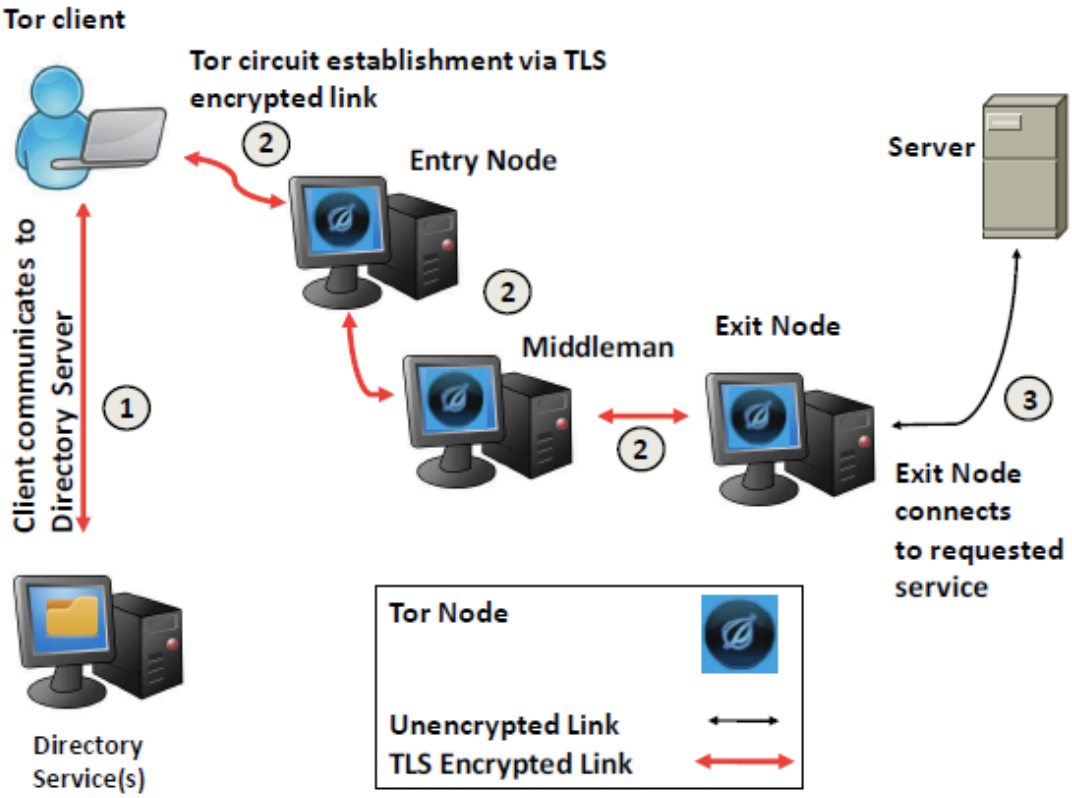


Fig. 24. Basic steps for communicating through TOR (Source: Khandelwal, 2014)

In addition to these methods, browser add-ons should also be mentioned. The internet browser add-ons are additional devices that are developed to enable the internet users in the third world to bypass government regulation and inspection to

promote free speech in the countries where free speech is not a full right or not exercised.

These advanced cyber methods provide influences that have implications for the nation state sovereignty, and in addition to these, using conventional cyber methods should also be added. Where and when the cyber ways fail for any purpose, resorting to conventional, more manual ways to curb state regulations is also a method. For instance, using outdated dial-up Internet connection during the Egyptian revolution after the authoritarian government shut down the main internet provision was a weak yet powerful channel and since it used the telephone lines, it was almost impossible for the government to hinder this.

These cyber methods might be thought to decrease the sovereignty of the states, but some other methods might also have direct advantageous effects on sovereignty. For instance, the capacity to shut down the Internet physically and thus thoroughly belongs to the nation states, since the physical infrastructure providing cyber services lie within the territories of the states and are connected in one way or another to a national regulation. Great Firewall practices rest solely within the hands of the nation states. These practices, the most renowned of which is the Golden Shield Project in China, that protects the internet traffic in and out, are rarely used but one of the most effective ways to confine the use of nation's cyberspace to its use only. In such a way, China was able to cut down the outside traffic, which it saw as a threat to its authoritarian one-party rule.

In addition, states have the capacity of Deep Package Inspection (DPI). DPI is a computer network packet filtering that is used to decide whether the packet may pass or if it needs to be routed to a different destination, or, for the purpose of collecting statistical information. In addition to using DPI for the security of their

own networks, governments in North America, Europe, and Asia use DPI for various purposes such as surveillance and censorship.

Companies selling system vulnerabilities to nation states that they can use to penetrate into the systems constitute a powerful tool in favor of the nation states, as well. The examples of these kinds of companies are VUPEN, GAMMA, etc., which were also on the news columns of major newspapers.

In addition to all these cyber features, an effective national security/safety discourse belongs to the nation states and they can effectively use it. It must be noted that the ability to produce a national security discourse regarding the cyberspace is a powerful reason for restricting freedoms on the Internet for nation states, just as it is an effective tool for conventional propaganda. Through dubbing the cyberspace as a domain where national security can be injured, restricting it, or at times, shutting it down wholesale, the state finds a way at its hands to consolidate its will ever more. The existence of the critical information system infrastructures is an important factor in this regard. It is a powerful tool at the hands of states that they own and control the critical information system infrastructure, and in the face of any potential threat to these systems, they can quite comfortably turn the issue into a national security concern and take measures as they see fit.

One of the most effective and famous ways of governments to restrict the content of the web, internet censorship can be carried out directly by the governments and or on behalf of them, by the private third party companies. With the rise and advance of more developed cyber methods, the number of states that limit access to Internet content has been on the rise in the recent years. The arguments of these states are like “securing intellectual property rights, protecting national security, preserving cultural norms and religious values” and “shielding children

from pornography and exploitation" (OpenNet Initiative, 2016). There are quite many cases of Internet censorship ranging from the authoritarian countries to the more liberal ones, and through various technical methods such as Internet Protocol (IP) blocking, Domain Name System (DNS) Filtering, URL Filtering, Packet Filtering or connection reset. The cases of the methods used and the governments using them confirm that these are a common way of restituting sovereignty vis-à-vis the non-state actors.

The securitization of the Internet, namely, that handling the Internet as a national security concern, as a matter that needs to be dealt with in the context of security and military, is one of the primary reasons of the regulation and the consolidation of sovereignty in the cyberspace. Though it is a space that has too many layers to be stuffed into solely one discourse such as security, the cyber space is regulated and discussed mostly by the security institutions and organizations, within the security discourse. Myriam Dunn Cavelty (2013) discussed this discourse of cyberspace as highly "securitized" throughout her article. She proposes that the cyberspace studies are exposed to too much militarization and securitization that it is now nearly impossible to conduct research regarding cyberspace without references to these phenomena, a factor that does not quite reflect the realities of the cyberspace (Cavelty, 2013). She recurrently argues that cyberspace is a zone that harbors more real and tangible threats such as cyber crimes or espionage, rather than cyber warfare in the hardcore military sense.

In addition to these cyber mechanisms, continuous monitoring of the Internet through fake SSL certificates is also an effective way through which an individual or institution can monitor the traffic of a network. SSL certificates are used to

authenticate secure encrypted Internet connections by binding an organization's identity, like a bank, to the appropriate domain name, server name, or host name.

As already mentioned, these cyber characteristics and cyber tools might have implications of some kind for the sovereignty of nation states and it is highly likely that we will witness some in the short or long term. They each beg for more detail research on the relationship between the cyberspace and political tenets of states. Especially the issue of regimes is significant. Though ignored deliberately in this thesis for academic convenience, regimes are an important independent variable that has results for the type of usage of the cyber world.

After looking at all the cases and some extra issues regarding cyberspace, it is now the time to move on to the last chapter of the thesis, namely, the Conclusion.

# CHAPTER 6

# CONCLUSION

"Why study cyberspace and, more specifically, why study cyberspace and sovereignty?" would be a proper question to ask, after having read the dozens of pages of this thesis, or even after reading the title of it. Cyberspace is not a quite popular topic with social scientists, and even less with political scientists, and there is only a handful of aficionados that are interested in analyses of cyberspace within the discipline of political science.

However, as this thesis firmly claimed in the cyberspace chapter previously, cyberspace is "the" technology of the twenty-first century, with an unprecedented capability of speed, efficiency and sustainability to it. There is hardly any country or society in the world as of now that is not dependent in some way on the cyberspace. The functioning of banks, state institutions, civil society, infrastructure, communication, healthcare and so on rely fully on the cyberspace, as well as the personal use of individuals.

The cyberspace being so vital to the contemporary life, in the discipline of political science, the literature regarding the cyberspace is extremely limited. As revealed by the literature review chapter of the thesis, the cyberspace literature is restricted to a few works and they mostly either argue that the sovereignty of the nation states are at risk due to the widespread use (in the future) of cyberspace and it will erode in the foreseeable future. On the other hand, the opposite camp argued that the cyberspace will be a handy tool of the states themselves and they will be even more sovereign in the future, giving enough evidence of their already doing so. However, the real problem with this cyberspace literature is that, it is extremely

outdated. It is stuck in the context of 1990s in which a hard battle was being fought between the leftist, Marxist camp and a neoliberal-oriented camp, with the latter seeming to win the battle at the time. The cyberspace use was definitely not widespread as it is now. As the literature was being written, only a few universities, military institutions and later, a handful of multinational companies, were able to use cyberspace. The hacking tools and incidents were not known; social media was not conceived of, and other features of cyberspace such as relative anonymity, mobility and efficiency of the cyberspace that developed after 2010s were not yet known to researchers. The analysts that studied cyberspace in that time focused on the fact that in the initial stages of cyberspace's development, it was a project of the public sector, with few prospects for private sector. This was the main reason of their reasoning that the cyberspace is the sovereignty-strengthening tool of the states, without knowing the futuristic use of cyberspace in monitoring citizen and non-state actor activities, which indeed immensely strengthened the sovereignty of states. The other group that insisted that the cyberspace is a tool that will erode state sovereignty argued so thinking that the private sector will take over some of the features enjoyed by sovereign states till that time. They were hardly aware that hacking will be a serious nuisance of the states in the close future, and some technical features of cyberspace will serve in order to erode cyberspace by different actors.

This is the exact reason that this thesis was written. It is intended to fill the large gap in cyberspace studies in political science with including the latest technical developments of cyberspace and their different uses by different actors. The thesis intends to be an updated cyberspace contribution into the discipline of political science and an initial study to encourage further research regarding the cyberspace.

The thesis employs the case study method and analyzes the eight cases that are chosen for their significance in portraying the influence of cyberspace on state sovereignty. While doing this, a crucial question arises: How to operationalize and measure the sovereignty and the effects of the cyberspace on sovereignty? After all, it was a fuzzy subject and an ephemeral concept. However, an operationalization scheme which was previously drafted by three scholars was used at this point, with ten indicators of a sovereign state. These ten functions of a sovereign state are legitimate monopoly on the means of violence, administrative control, management of public finances, investment in human capital, delineation of citizenship rights and duties, provision of infrastructure services, formation of the market, management of the state's assets (including the environment, natural resources, and cultural assets), international relations (including entering into international contracts and public barrowing) and the rule of law. Each case study in the thesis looks into the background of the concerned case first, and afterwards, analyzes which one(s) of these sovereign state functions are affected due to the cyberspace use and how.

The cases that exemplify the erosion of state sovereignty are six in number and they all illustrate a different case process with different actors that used distinct methods. The first case, Bitcoin, is a case in which the monetary sovereignty of the states in the contemporary world is challenged due to a cyber monetary transaction unit named as Bitcoin. Printing paper money or issuing coins have always been the most direct symbol of sovereign states and Bitcoins that are used effectively on the cyberspace challenge this very monopoly of the states, by not being subject to the regulations of a central bank, by running out of legal monetary circling, by not being tractable in any conventional way. The fear over the lack of governmental control over the use and production of Bitcoin led quite many states in the world to take

necessary actions against Bitcoin, which in theory at least, are not effective against the use of Bitcoin. The provisions of the FBI report regarding the use of Bitcoin clarify the ways in which Bitcoin challenges many aspects of the sovereignty of a state. Bitcoin is highly likely to be used for illegal purposes which would normally not be conducted under the regular monetary scheme of the states, besides being an ample ground for Bitcoin thefts, malicious transactions due to the lack of records of the cyber currency. The case of Bitcoin thus gives us an example in which not only one specific state is challenged in terms of its sovereignty practices, but rather, all of the states on the globe are in the range of Bitcoin's challenge. It is also a case in which the sovereignty-eroder actor is not a specific group or an institution, or another state, as the other cases entail. In the Bitcoin case, the sovereignty-eroder actors are firstly the cyber group that allowed the functioning of the cyber currency by setting up the "mining" platform for the "production" of the Bitcoin. Secondly, the sovereignty-eroder actor in this Bitcoin case involves the masses of individuals and groups that actively use the cyber currency and thus curb state's monetary monitoring and control, which directly or indirectly erodes the sovereignty of state(s) in question. This type of a sovereignty-eroder is different from the equivalent actors in other cases, where the sovereignty-eroder actors are either a single hacker group, another state or masses of demonstrators. Bitcoin case, rather interestingly, also supports the arguments of the leftist political science analysts, mentioned in the literature review, who hold that the "actors" (they mostly thought these actors to be private sector) could take over the economic sovereignty practices of nation states and thus erode state sovereignty. However they were not able to envisage that an alternative currency would replace the legally acceptable currencies authorized by the sovereign states.

The second case, namely, the Russian Dominance of Ukrainian cyberspace case, is a clear example of a state's sovereignty erosion due to the active cyberspace use of another state. Russia, a country known for its active presence in the cyberspace, supported the Russian hacker groups to take over the control of the Ukrainian cyber facilities during the pro-Russian unrest in the country and the annexation of Crimea in 2014. While the ground insurgencies in Ukraine were continuing, the Russian cyber activities helped the Russian cause. This dominance took place using a multitude of platforms and methods, like the disabling of the IXP that connected the Crimean Peninsula to the Ukrainian mainland. The official Ukrainian websites were hacked and the news of the violation of the ceasefire by the Ukrainian side were posted, which effectively curbed the sovereignty of the Ukrainian state. The case illustrates a situation in which a state's legitimate monopoly on the means of violence, its administrative control, its capability to deliver infrastructure services, its ability to enter into international relations as it wills and its ability to provide rule of law are negatively affected. It must be noted once again that the actor in this case is another state vis-à-vis the "victim" state.

The third case, namely the Stuxnet case is similar to the previous one in terms of the actor: another state. However, the Stuxnet case differs from other cases in that Stuxnet is a malicious software that was specifically designed by a state for the prevention of the nuclear program of another state, the US and Iran respectively. As both the technical and political reports regarding Stuxnet indicate, it was developed by the US and tested in a model nuclear plant in Israel, and was ultimately sent over to the Natanz nuclear facility through a contractor company. Due to this cyber weapon, the target of Stuxnet, namely the Natanz nuclear plant, had to postpone its nuclear enrichment program for at least two years, during which the Stuxnet secretly

operated on the aforementioned nuclear plant without being caught by the Iranian control authorities. Stuxnet was therefore able to hinder Iran's monopoly on the means of violence, its ability to manage its public finances, its ability to provide infrastructure services and its capability to manage its own assets (which, in this case, is the nuclear assets). These points all clearly demonstrate that the Iranian state's sovereignty got severely eroded in these aspects due to the use of cyberspace by another state. The Stuxnet case, since it is the first recorded cyber weapon in history, also gives the researchers the chance to analyze how a futuristic weapon might function and have an influence on a state, on which there is a present gap in international law regarding how to respond to such offensives in the future. Stuxnet cyber weapon, therefore, is one of the most direct cases in which a state is behind the sovereignty erosion of another state through the cyberspace.

The fourth case, the Egyptian Revolution, is another case in which the sovereignty of a state was eroded due to cyberspace. This case differs from the two previous cases in that, the actor that led to the Egyptian state's sovereignty erosion is not another state, but the masses of cyberspace users. The aftermath of the Arab Spring that swept the entire Middle East also affected Egypt and the masses poured onto the major streets in historic demonstrations and rallies against the authoritarian Mubarak regime. Mass protests that erupted on 25 January 2011 resulted in harsh measures from the regime, but the masses that communicated over the cyberspace were able to reach millions in number, which soon turned into a movement impossible to be contained by the regime. Cyberspace was the primary reason of mobilization in all these processes, in a country and political setting where it was impossible to get mobilized in the past and cyberspace granted the masses the ability to mobilize with speed and anonymity. Due to these features of cyberspace

mobilization, the Mubarak government was soon overthrown. Egyptian state's administrative control, its ability to delineate its citizens' rights and duties, its ability to provide infrastructure services during the mass protests and its ability to maintain a rule of law all got severely impaired due to the heavy use of cyberspace, and it can be safely argued that the sovereignty of the Egyptian state got eroded.

The fifth case is the 2014 Sony Pictures Entertainment Co. Hacking incident, and the case resembles the Stuxnet and the Russian Dominance of Ukrainian Cyberspace cases since a state is behind the erosion of sovereignty of another state in this case as well. The hacking incident took place when the Sony Pictures Entertainment Co. announced its intention to release a comedy movie called *The Interview*, whose subject is the assassination of the North Korean totalitarian leader. The Republic of North Korea strongly and obsessively protested this through various channels and threatened to retaliate back if the company did not stop the movie project. In 2014, North Korean linked hacker groups hacked Sony Entertainment Co, leaked all of the sensitive data regarding the company's future projects and financial information, resulting in the loss of millions of dollars on the part of the entertainment company. The cyber incident caused the company to take a step back and to ultimately decide not to release the movie on theatres. The US government, having felt humiliated in the face of North Korea, responded to the decision of the company rather negatively, and the situation turned into a diplomatic incident that involved the US state. As a result of the hacking incident, the US's administrative control capabilities, its ability to manage its assets (in this specific case, cultural assets), its ability to bargain some issues in its international relations got negatively affected. The negatively affected sovereignty indicators indicate that the US sovereignty is eroded in these aspects due to the use of cyberspace by North Korea.

The sixth case is the RedHack case and it is the last case in the thesis that sovereignty erosion is in question. The RedHack case is a relatively minor one, when it is compared with other cases, since its effects were minimal. The sovereignty-eroder actor in this case is not a state or masses, as in the previous cases, but a leftist-oriented hacker group called RedHack. The group attacked the websites of various state institutions to protest against the acts of the government, particularly acts against freedom of expression. The group hacked and posted propaganda materials on the official websites, and, leaked massive amounts of secret state information in order to reveal the weaknesses of the institutions. As a result of the various hacking incidents of RedHack, the Turkish state's administrative control capabilities, its ability to manage its own assets (in this case, the cyber assets such as websites and digital information), and its rule of law were negatively affected and its sovereignty was eroded in terms of these specific aspects.

These cases were the ones in which the sovereignty of a state got eroded due to the cyberspace use. The next two cases that are classified under the "Sovereignty Strengthened" group are the ones in which the sovereignty of the states are strengthened due to their own efficient use of the cyberspace.

First of these two cases is the Great Firewall of China, which focuses on the cyber measures of the Chinese state against the freedom of expression of the opponent groups and against other states' possible influence in China. China controls the web content that its citizens has access to, together with all the cyber activities going on cyberspace. The method of achieving this is multiple: Firstly, Chinese institutions responsible for cyber control create the Chinese alternatives of the globally popular platforms such as Google, Facebook or Twitter and cut the access to these global websites from within. Secondly, through the Golden Shield Project, a

censorship and surveillance mechanism, the Chinese state blocks the data that comes from outside of China which is deemed not appropriate for the Chinese cyber users. Thirdly, a human layer is also used by the Chinese state. State officials and cyber-volunteers monitor the Chinese cyberspace for any unsuitable content. Fourthly and lastly, Chinese state uses cyberspace as a fertile ground for its own state propaganda, which contributes to its sustainability even more. As a result of the use of cyberspace by the Chinese state, its legitimate monopoly on the means of violence, its administrative control ability, its capability to delineate its citizens' rights and duties, its ability to manage its assets and its capability of maintaining a rule of law in the country are all immensely strengthened. These sovereignty indicators demonstrate that the Chinese state's sovereignty is strengthened due to its use of cyberspace.

The second of the two cases is the NSA Cyber Practices as revealed to the public by the Snowden case. The National Security Agency practices ongoing on the cyberspace were leaked to the public in 2013 and it was revealed that the US state was quite active on cyberspace and actively pursuing the endeavors to both monitor, control and manipulate the cyber activities all around the world. Getting the private communication information of the US citizens from communication companies, collecting private information from social media websites by creating access to their servers, spying on numerous world leaders and other countries' citizens, trying to break online privacy and encryption tools that the cyber users might choose to use for anonymity purposes, breaking into the databases of technology giants and trying to collect telephone call information from any country that the NSA wishes are among the cyber practices of the NSA on cyberspace. This massive amount of cyber activities of the NSA contributed to the administrative control capabilities of the US, its ability to delineate its citizens' rights and duties effectively, its ability to manage

its international relations and its capabilities in maintaining the rule of law, which, in turn, shows that the cyberspace use strengthened the sovereignty of the US.

The six cases that are listed above under the "Sovereignty Eroded" subtitle are the ones that a kind of sovereignty erosion of a state is analyzed case. The last two cases that are classified under the "Sovereignty Strengthened" group are the ones in which the sovereignty of the states is strengthened due to their own efficient use of the cyberspace.

All the cases collected above demonstrate that the cyberspace is not a platform or a tool that solely strengthens the sovereignty of the states, as one camp of the existing cyberspace literature claimed previously. This literature, as analyzed in the literature review section of the thesis, is divided into two strict and mutually exclusive camps that either argue the strengthening of state sovereignty or the erosion of it due to the novel technology. The cyberspace, rather than merely doing one of these two, is suitable for both: it can strengthen the sovereignty of a state as well as do the opposite and the primary reason for this difference lies with some other factors that need more research. For instance, regime type (which this thesis ignores) might be a strong factor that determines how a state is going to interact with the cyberspace.

By analyzing each case, the thesis contributes immensely to the cyberspace literature that was stuck in 1990s. In addition, the recent technical features of cyberspace that have been used since 2010s are also reviewed in a political science study for the first time. It primarily lays down the fact that the relationship between cyberspace and sovereignty is complex, deep, multi-layered and it begs for detailed studies and research that take into account the vast and multiple technical methods or features offered by cyberspace in the recent years. In the light of these cases in the

thesis, the geometry and shape of the relationship between the sovereign states, non-state actors and other sovereign states are in a process of a constant change.

The analyses regarding the cyberspace not only give us insights regarding the cyberspace itself; but rather, they provide us in-depth novel data to understand sovereignty in a wholly new perspective. One line of thinking might suggest that the cyberspace brings in totally new changes (and challenges) to the historical descriptions of sovereignty. The fact that the cyberspace has a nature that cannot be physically located, that it is far away from having a solely material existence that it thus cannot be conceived within the strict borders of a sovereign nation state lead slightly to the erosion of the distinction between "internal sovereignty" and "external sovereignty" in the sovereignty literature. The cyberspace renders these sovereignty distinctions and descriptions rather obsolete. The reason for this is that, due to the cyberspace, the very distinction between what is really internal and what is really external for a state is blurred to an extent, which in turn affects the understanding of the term sovereignty itself. For instance, as can be remembered from the sovereignty chapter, the distinction between the "Vettalian sovereignty" and "Westphalian sovereignty", two categories according to Krasner's sovereignty description scheme, is blurred and these two sovereignty types are intertwined. In the same way, the main components and aspects of the term "sovereignty", such as internal sovereignty, external sovereignty or the direct sovereignty indicators are questionable in the aftermath of the development of cyberspace.

It can be safely argued that the conventional sovereignty conception in which the state is thought to be different and distinct from the non-state actors and other states and where "the sovereign state" regulates the relations and duties between them is challenged by the cyberspace. If we have to define it in more philosophical

and hypothetical terms, we witness a sovereignty context where the "sovereign" state is less in a hierarchical relationship with the non-state actors under it, but functions at times more like a non-state actor itself in the cyberspace. What is certainly visible is that the concept sovereignty turns into a phenomenon more complex and more entailing soft-power from the directly harsh hierarchical top-down relational concept. The "territoriality" component of the concept sovereignty disappears and a sovereignty understanding that can exist without "being sovereign on a piece of territory", without a specific ontological territory is on the way. Sovereignty, in its new form, seems to be more fluid and ethereal, a concept that needs more attention to see in rather different practices.

However, regarding cyberspace, for those who still maintain a realist view of the sovereignty concept, all the technological means, cyberspace included, are just handy tools of state sovereignty and they constitute the new ways through which the state can infiltrate into the previously untouched areas of human lives. For them, the cyberspace, with sharply reduced costs and time required for the transport of goods (and services), and similar reductions in costs and time requirements for communication, is especially suitable for this kind of strengthening of state sovereignty. Though this group is a persistent one, some aspects of a sovereign state, such as money-printing which is a direct symbol of sovereignty, seem to erode due to the use of cyberspace, as analyzed in the Bitcoin case. Does cyberspace in a way promise to bring about a wholly different and novel type of sovereignty understanding for states? Which aspects of sovereignty are more prone to the technological advances like cyberspace and which aspects seem to be steadfast in the face of them? These questions still remain open to research and more thorough contemplation.

This thesis is a humble attempt to contribute to the cyberspace and sovereignty literature, which has been left aside for nearly two decades. Besides trying to analyze the latest features and tools of cyberspace, a vital technology of today, it delves into the nature and challenges of the concept "sovereignty" in the contemporary times. The gap to which the thesis addresses is too wide to be filled with only one work and the cyberspace studies need more research, both in terms of quality and quantity. An ever-expanding and immensely vast space such as cyberspace might defy any social science research being conducted over it, with restricted literature to benefit from, with difficulties regarding the nature and actors on this new "space", with methodological and epistemological hardships for scholars trying to study cyberspace.

But it is surely worth it.

REFERENCES


Abass, A. (2001). *The complete international law: text, cases, and materials*. Oxford: Oxford University Press.

Agnew, J. A. (1987). *Place and politics: The geographical mediation of state and society*. Boston: Allen & Unwin.

Alexander, A. (2011, February 9). Internet role in Egypt's protests. *BBC News*. Retrieved from http://www.bbc.com/news/world-middle-east-12400319

Alluned. (n.d.). *Bitcoin*. Retrieved from http://www.alluned.com/bitcoin/

Anghie, A. (1999). Finding the peripheries: Sovereignty and colonialism in nineteenth-century international law. *Harvard International Law Journal*, *40*(1), 1-80.

Atis Telecom Glossary. (2016). Retrieved from http://www.atis.org/glossary/definition.aspx?id=6555

Barlow, J. P. (1990). *Crime and puzzlement*. Retrieved from https://w2.eff.org/Misc/Publications/John_Perry_Barlow/HTML/crime_and_puzzlement_1.html

Barlow, J. P. (1996). *A declaration of the independence of cyberspace*. Retrieved from https://www.eff.org/cyberspace-independence

Beaumont-Thomas, B. (2014, July 10). North Korea complains to UN about Seth Rogen comedy The Interview. *The Guardian.* Retrieved from http://www.theguardian.com/film/2014/jul/10/north-korea-un-the-interview-seth-rogen-james-franco

Betz, D. & Stevens, T. (2012). *Cyberspace and the state: Toward a strategy for cyber-power*. London, U.K.: City: Routledge.

Bitcoin Bank GL. (n.d.). Retrieved from http://www.bitcoinbank365.com/all-about-bitcoin

Boyd, E. B. (2011, January 31). *How social media accelerated the uprising in Egypt*. Retrieved from http://www.fastcompany.com/1722492/how-social-media-accelerated-uprising-egypt

Brito, J. & Castillo, A. (2016). *Bitcoin: A primer for policymakers*. Arlington, VA: Mercatus Center.

Cairncross, F. (2001). *The death of distance: How the communications revolution is changing our lives*. Boston, MA: Harvard Business School Press.

Can, M. (2014a, May 15). *Stuxnet and international law: Possible scenarios*. Retrieved from http://www.turkishweekly.net/2014/05/15/op-ed/stuxnet-and-international-law-possible-scenarios/

Can, M. (2014b, June 23). *A cyber 'axis of evil'? : A short exploration of 'cyberchallenging' the international order*. Retrieved from http://www.turkishweekly.net/2014/06/23/op-ed/a-cyber-axis-of-evil-a-short-exploration-of-cyberchallenging-the-international-order/

Chebib, K. N. & Sohail, R. M. (2011). The reasons social media contributed to the 2011 Egyptian revolution. *International journal of business research and management (IJBRM)*, *2*(3), 139-162.

Chen, G., Dickinson, S., Schlesinger, D., Qiang, X., Creemers, R., & Wertime, D. (2015, February 3). China's great firewall is rising: technology and political will are converging to create a seamless nationwide intranet – amid growing netizen anger. *Foreign Policy*. Retrieved from http://foreignpolicy.com/2015/02/03/china-great-firewall-is-rising-censorship-internet/

China Internet Network Information Center. (2006). *17th statistical survey report on the Internet development in China*. Retrieved from http://www.cnnic.net.cn/download/2006/17threport-en.pdf

Clark, D. (2010, March 12). Characterizing cyberspace: past, present, and future. *ECIR Working Papers*. Retrieved from http://ecir.mit.edu/index.php/research/working-papers/112-characterizing-cyberspace-past-present-and-future

Crimson Hexagon. (2016). *Egyptian social media analysis reveals nation's perspectives on election*. Retrieved from http://www.crimsonhexagon.com/blog/current-events/egyptian-social-media-analysis-election/

Crofton, I. (2015). *Crypto Anarchy*. Raleigh, NC: Lulu Press.

Cumhuriyet. (2012, April 20). RedHack İçişleri'ne takla attırdı. *Cumhuriyet*. Retrieved from http://www.cumhuriyet.com.tr/haber/diger/336388/RedHack_icisleri_ne_takla_attirdi_.htm

Currie, J. (2015, March 16). The 2011 Egyptian Revolution and the role of social media. *Geographies of the Middle East*. Retrieved from http://megeog.org/2015/03/16/the-2011-egyptian-revolution-and-the-role-of-social-media/

Cyberspace Law and Policy Community. (2014, April 24). *Law in the information age: cybercrime*. Retrieved from http://www.cyberlawcentre.org/genl0231/crime.htm

Danmarks Nationalbank. (2014, March 18). *Bitcoins are not money* [Press Conference]. Retrieved from http://www.nationalbanken.dk/en/pressroom/Documents/2014/03/Presshistory_Bitcoins_UK.pdf

Daunt, T. & Szalai, G. (2015, January 13). White House Unveils Proposal for Cybersecurity Legislation in Wake of Sony Hack. *Hollywood Reporter*. Retrieved from http://www.hollywoodreporter.com/news/white-house-unveils-proposal-cybersecurity-763269

Deibert, R. (2013). *Black code: Inside the battle for cyberspace*. Toronto: McClelland & Stewart.

Democracy Now. (2014, December 23). *U.S. rejects North Korea's 'Absurd' Call for Joint Probe of Sony Hack*. Retrieved from http://www.democracynow.org/2014/12/23/headlines/us_rejects_north_koreas_absurd_call_for_joint_probe_of_sony_hack

Department of Defense. (2006, December). *National Military Strategy for Cyberspace Operations*. Retrieved from http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-023.pdf

Dictionary.com. (2015). "domain" in *The Dictionary.com*. Retrieved from http://dictionary.reference.com/browse/domain

Dunn-Cavelty, M. (2013). From cyber-bombs to political fallout: threat representations with an impact in the cyber- security discourse. *International Studies Review*, *2013*(15), 105-122. Retrieved from https://www.researchgate.net/profile/Myriam_Dunn_Cavelty/publication/251347497_From_Cyber-Bombs_to_Political-Fallout_Threat_Representations_with_an_Impact/links/0f317537c59561ad60000000.pdf

Ebert, H. & Maurer, T. (2013). Contested cyberspace and rising powers. *Third World Quarterly*, *34*(6), 1054-1074.

Economist. (2013, April 6). Special report: the Great Firewall: the art of concealment. *The Economist*. Retrieved from http://www.economist.com/news/special-report/21574631-chinese-screening-online-material-abroad-becoming-ever-more-sophisticated

England, G. (2009). *Memo from the Deputy Secretary of Defense*. Retrieved from https://www.nsa.gov/public_info/speeches_testimonies/5may09_dir.shtml

FBI. (2012, April 24). *Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity [Federal Bureau of Investigation Intelligence Assessment]*. Retrieved from https://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf

Finkle, J. (2014, October 14). Russian hackers target NATO, Ukraine and others: iSight. *Investing Technology News.* Retrieved from http://www.investing.com/news/technology-news/russian-hackers-target-nato,-ukraine-and-others:-isight-312945

Franceschi-Bicchierai, L. (2014, June 5). The 10 biggest revelations from Edward Snowden's leaks. *Mashable*. Retrieved from http://mashable.com/2014/06/05/edward-snowden-revelations/

Frizell, S. (2015, February 4). Sony is spending $15 million to deal with the big hack. *Time*. Retrieved from http://time.com/3695118/sony-hack-the-interview-costs/

Fukuyama, F. (1989). *The end of history*. Washington, D.C.: National Affairs.

Ghani, A., Lockhart, C. & Carnahan M. (2005). *Closing the sovereignty gap: An approach to state-building*. London, U.K.: Overseas Development Institute.

Gibson, W. (1984). *Neuromancer.* New York: Ace Books.

Gingrich, N. (2014, December 18). America lost the cyberwar over Sony: Now what?. *CNN Online*. Retrieved from http://edition.cnn.com/2014/12/18/opinion/gingrich-america-lost-cyberwar-sony/

GlobalWebIndex. (2015). GlobalWebIndex's quarterly report on the latest trends in social networking. *GWI Social Summary, Q1*(2015). Retrieved from https://www.globalwebindex.net/hs-fs/hub/304927/file-2812772150-pdf/Reports/GWI_Social_Summary_Report_Q1_2015.pdf

Goldsmith, J. L. (1998). The Internet and the abiding significance of territorial sovereignty. *Indiana Journal of Global Legal Studies, 5*(2). 475-491.

Goldsmith, J. L., & Wu, T. (2006). *Who controls the Internet? Illusions of a borderless world*. New York: Oxford University Press.

Graham, M. (2013). Geography/Internet: Ethereal alternate dimensions of cyberspace or grounded augmented realities?. *The Geographical Journal*. *179*(2), 177-188.

Griffiths, J. (2015, October 26). Great Firewall rising: How China wages its war on the Internet. *CNN*. Retrieved from http://edition.cnn.com/2015/10/25/asia/china-war-internet-great-firewall/

Gunst, P. (2015, February 9). *Bitcoin*. Retrieved from https://www.lawgives.com/guide/5423423377777744aa010000/Bitcoin

Hare, F. (2011). *Borders in cyberspace: Can sovereignty adapt to the challenges of cyber security?*. Tallinn: NATO Cooperative Cyber Defense Center of Excellence Publication. Retrieved from https://ccdcoe.org/publications/virtualbattlefield/06_HARE_Borders%20in%20Cyberspace.pdf

Hafner, K. (1998). *Where wizards stay up late: The origins of the Internet*. New York: Simon & Schuster.

Harris, S. (2014, May 3). Beware the Russian cyber bear. *Pittsburgh Post-Gazette*. Retrieved from http://www.post-gazette.com/opinion/Op-Ed/2014/05/04/lt-div-class-libPageBodyLinebreak-gt-The-Russian-cyber-bear-lt-div-gt/stories/201405040018

Harwit, E. & Clark, D. (2001). Shaping the Internet in China: Evolution of political control over network infrastructure and content. *Asian Survey, 41*(3), 337-408.

Hathaway, M. (2014). Connected choices: How the Internet is challenging sovereign decisions. *American Foreign Policy Interests*, *36*(5), 300–313. Retrieved from http://belfercenter.ksg.harvard.edu/files/uafp_a_969178_hathaway.pdf

Hayek, F. (1976). *The denationalization of money: The argument refined*. London: Inst. of Economic Affairs.

Henkin, L. (1999). That "S" word: Sovereignty, and globalization, and human rights, et cetera. *Fordham Law Review, 68*(1), 1-14. Retrieved from http://ir.lawnet.fordham.edu/flr/vol68/iss1/1

Henwood, D. (2014, May 19). Is Bitcoin the future of money?: libertarians and leftists alike predict a world of competing digital currencies. *The Nation*. Retrieved from https://www.coursehero.com/file/13023987/677/

Hesseldahl, A. (2014, November 28). Sony Pictures investigates North Korea link in hack attack. *Re/code*. Retrieved from http://recode.net/2014/11/28/sony-pictures-investigates-north-korea-link-in-hack-attack/

Homeland Security. (2008, January 8). *Homeland Security Presidential Directive HSPD-23*. Retrieved from https://fas.org/irp/offdocs/nspd/nspd-54.pdf

House of Lords Decision. (1939). *The Arantzazu Mendi Case*. 1939-A. C. 256.

Hurriyet Daily News. (2012, July 3). RedHack discloses IDs of foreign diplomats in Turkey. *Hurriyet Daily News*. Retrieved from http://www.hurriyetdailynews.com/redhack-discloses-ids-of-foreign-diplomats-in-turkey-.aspx?pageID=238&nID=24617&NewsCatID=374

ICANN. (2016). *Bylaws for Internet Corporation for Assigned Names and Numbers*. Retrieved from https://www.icann.org/resources/pages/governance/bylaws-en

Ignatius, D. (2014, February 5). After Snowden a diminished Internet. *Washington Post*. Retrieved from https://www.washingtonpost.com/opinions/david-ignatius-after-snowden-a-diminished-internet/2014/02/05/59ea1784-8e89-11e3-b227-12a45d109e03_story.html

International Court of Justice. (1949). *Corfu Channel Case*. UK v. Alb. 1949 I.C.J. 39, 43.

International Telecommunications Union. (2013, July). *Percentage of individuals using the Internet 2000-2012*. Retrieved from https://www.itu.int/en/ITU-D/Statistics/Documents/.../Individuals_Internet_2000-2012.xls

Island of Palmas Case. (1926). Island of Palmas case (U.S. v. Netherlands), 2 R. *International Arbitrary Awards 821* (838) (1928).

ISC. (2016). *Internet systems consortium history*. Retrieved from https://www.isc.org/solutions/survey/history

Johnson D. R. & Post, D. G. (1996). Law and borders: the rise of law in cyberspace. *Stanford Law Review, 48*(1367). Retrieved from https://cyber.law.harvard.edu/is02/readings/johnson-post.html

Jiang, X. (2008, November 24). How China's Internet police control speech on the Internet. *Radio Free Asia*. Retrieved from http://www.rfa.org/english/commentaries/china_internet-11242008134108.html

Kelley, M. B. (2013, November 20). The Stuxnet attack on Iran's nuclear plant was 'far more dangerous' than previously thought. *Business Insider*. Retrieved from http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11

Khandelwal, S. (2014, November 18). 81% of TOR users can be easily unmasked by analysing router information. *The Hacker News*. Retrieved from http://thehackernews.com/2014/11/81-of-tor-users-can-be-easily-unmasked_18.html

Krasner, S. D. (2001). Abiding sovereignty. *International Political Science Review / Revue internationale de science politique, 22*(3), 229-251.

Kubra, H. (2012, June 25). Redhack internetin fişini yine çekecek mi?. *InternetHaber*. Retrieved from http://www.internethaber.com/twit-ul-havadis-internethaber-hatice-kubra-redhack-soylesi-eylem-redhacktime-htc-437607h.htm?interstitial=true

Kuehl, D. T. (2009). From cyberspace to cyberpower: defining the problem. In F. D. Kramer, S. H. Starr, & L. K. Wentz (Eds.), *Cyberpower and national security*. Washington, D.C: Center for Technology and National Security Policy. Retrieved from http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-02.pdf

Kushner, D. (2013, February 26). *The real story of Stuxnet*. Retrieved from http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

Langner, R. (2013, November 19). Stuxnet's secret twin. *Foreign Policy*. Retrieved from http://foreignpolicy.com/2013/11/19/stuxnets-secret-twin/

Laughland, O. & Rushe, D. (2014, December 20). Sony pulling The Interview was 'a mistake' says Obama. *The Guardian*. Retrieved from http://www.theguardian.com/us-news/2014/dec/19/obama-sony-the-interview-mistake-north-korea

Legal Information Institute. (n.d.) 'currency' definition. Retrieved from https://www.law.cornell.edu/definitions/index.php?width=840&height=800&iframe=true&def_id=2ba1b07652737e61dd887dbccf1e8cc4&term_occur=15&term_src=Title:31:Subtitle:B:Chapter:X:Part:1010:Subpart:A:1010.100

Lennon, M. (2014, December 19). Hackers used sophisticated SMB worm tool to attack Sony. *SecurityWeek*. Retrieved from http://www.securityweek.com/hackers-used-sophisticated-smb-worm-tool-attack-sony

Linfo. (2005). 'computer network' definition. *Linfo*. Retrieved from http://www.linfo.org/network.html

Living Internet. (2015). Interface message processor. *Living Internet Commons*. Retrieved from http://www.livinginternet.com/i/ii_imp.htm

Maheshwari, V. (2015, February 18). Ukraine's lonely cyberwarrior vs. Russia. *The Daily Beast*. Retrieved from http://www.thedailybeast.com/articles/2015/02/18/ukraine-s-lonely-cyber-warrior.html

Martin-Vegue, T. (2015a, March 24). Cyber what?. *CSO Online*. Retrieved from http://www.csoonline.com/article/2900300/cyber-attacks-espionage/cyber-i-what-i-part-1-of-2.html

Martin-Vegue, T. (2015b, April 24). Are we witnessing a cyber war between Russia and Ukraine? Don't blink - you might miss it. *CSO Online*. Retrieved from http://www.csoonline.com/article/2913743/cyber-attacks-espionage/are-we-witnessing-a-cyber-war-between-russia-and-ukraine-dont-blink-you-might-miss-it.html

Mathews, J. T. (1997, January/February). Power shift. *Foreign Affairs, 76*(1), 50-66.

Mesoznik, K. (2015, November 10). The ins and outs of the Great Firewall of China. *The Huffington Post*. Retrieved from http://www.huffingtonpost.com/karen-mesoznik/the-ins-and-outs-of-the-g_b_8510918.html

Milliyet. (2012, February 14). Aile Bakanlığı'nı RedHack hackledi. *Milliyet*. Retrieved from http://www.milliyet.com.tr/aile-bakanligi-ni-redhack-hackledi/gundem/gundemdetay/14.05.2012/1539999/default.htm

Morozov, E. (2011). *The net delusion: The dark side of Internet freedom*. New York, NY: PublicAffairs.

Müller, M. (2013). *Networks and states: The global politics of Internet governance*. Cambridge, MA: MIT Press.

Naidoo, K. (2000, April 20). The new civic globalism. *The Nation*. Retrieved from https://www.thenation.com/article/new-civic-globalism/

New Internationalist. (2016). World development book case study: The role of social networking in the Arab Spring. *New Internationalist.* Retrieved from http://newint.org/books/reference/world-development/case-studies/social-networking-in-the-arab-spring/

Ntvmsnbc. (2013). Şifre aynı: 123456. *Ntvmsnbc*. Retrieved from http://www.ntvmsnbc.com/id/25414019

Nye, J. (2014, June). Interview with Joseph Nye. *Analist*. Retrieved from http://www.analistdergisi.com/sayi/2014/06/joseph-nye

Ocak, S. (2012, March 30). 'Tutuklu' RedHack 350 siteyi hackledi. *Radikal*. Retrieved from http://www.radikal.com.tr/turkiye/tutuklu_redhack_350_siteyi_hackledi-1083334

Open Technology Institute. (2015). *Compilation of existing cybersecurity and information security related definitions*. Washington D.C.: Open Technology Institute of New America.

OpenNet Initiative. (2005, April 14). *Internet filtering in China 2004-2005: A country study*. Retrieved from http://www.opennetinitiative.net/studies/china/

OpenNet Initiative. (2016). *About filtering*. Retrieved from https://opennet.net/about-filtering

Oppenheim, L. & Roxburgh, S. R. (1920). *International law, a treatise.* London: Longmans, Green and Co.

Oppliger, R. (2014). *Secure messaging on the Internet*. Norwood, MA: Artech House.

Pagliery, J. (2014, December 29). 'Sony-pocalypse': Why the Sony hack is one of the worst hacks ever. *CNN Money*. Retrieved from http://money.cnn.com/2014/12/04/technology/security/sony-hack/

Pauli, D. (2013, November 22). Deadly ninja Stuxnet the first to attack Iran nuclear plant. *IT News*. Retrieved from http://www.itnews.com.au/news/deadly-ninja-stuxnet-the-first-to-attack-iran-nuclear-plant-365124#ixzz42Vjnl7s2

Peck, M. (2013). Did Anonymous hack Israel's Mossad spy agency?. *Forbes*. Retrieved from http://www.forbes.com/sites/michaelpeck/2013/03/24/did-anonymous-hack-israels-mossad-spy-agency

People's Daily Online. (2010, June 8). *The Internet in China*. Retrieved from http://en.people.cn/90001/90776/90785/7017177.html

Perritt, H. H. (1998). The Internet as a threat to sovereignty? Thoughts on the Internet's role in strengthening national and global governance. *Indiana Journal of Global Legal Studies, 5*(2), 423-442.

Post, D. G. (2009). *In search of Jefferson's moose: Notes on the state of cyberspace*. Oxford: Oxford University Press.

Postel, J. (n.d.) *Arpanet Map*. Retrieved from https://en.wikipedia.org/wiki/History_of_the_Internet#/media/File:Internet_map_in_February_82.png

Postel, J. (1981). *NCP/TCP transition plan*. Retrieved from https://tools.ietf.org/html/rfc801

Qiang, X. (2008, November 24). How China's Internet police control speech on the Internet. *RFA*. Retrieved from http://www.rfa.org/english/commentaries/china_internet-11242008134108.html

Radikal. (2013, January 21). Redhack'ten 'terörist değiliz' tepkisi. *Radikal*. Retrieved from http://www.radikal.com.tr/turkiye/redhackten_terorist_degiliz_tepkisi-1117856

Riley, M. (2015, October 14). Cyberspace becomes second front in Russia's clash with NATO. *Bloomberg*. Retrieved from http://www.bloomberg.com/news/articles/2015-10-14/cyberspace-becomes-second-front-in-russia-s-clash-with-nato

Rivera, J. (2014, March 2). Has Russia begun offensive cyberspace operations in Crimea?. *Georgetown Security Studies Review*. Retrieved from http://georgetownsecuritystudiesreview.org/2014/03/02/has-russia-begun-offensive-cyberspace-operations-in-crimea/

Ross, A. (2014, March 12). Russia's cyber weapons hit Ukraine: How to declare war without declaring war. *The Christian Science Monitor*. Retrieved from http://www.csmonitor.com/Commentary/Global-Viewpoint/2014/0312/Russia-s-cyber-weapons-hit-Ukraine-How-to-declare-war-without-declaring-war

Rothrock, K. (2014, April 9). Kremlin's digital gulag. *Moscow Times*. Retrieved from http://www.themoscowtimes.com/opinion/article/the-kremlins-digital-gulag/497809.html

Rushe, D. (2014, February 27). Janet Yellen: Federal Reserve has no authority to regulate Bitcoin. *The Guardian*. Retrieved from https://www.theguardian.com/business/2014/feb/27/janet-yellen-federal-reserve-no-authority-regulate-bitcoin

Sanger, D. (2012, June 1). Obama order sped up of wave of cyberattacks against Iran. *New York Times*. Retrieved from http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=0

Sanger, D. & Perlroth, N. (2014, December 17). U.S. links North Korea to Sony hacking. *The New York Times*. Retrieved from http://www.nytimes.com/2014/12/18/world/asia/us-links-north-korea-to-sony-hacking.html

Sassen, S. (1998). On the Internet and sovereignty. *Indiana Journal of Global Legal Studies*, *5*(2), 545-559.

Seal, M. (2015, February 4). An exclusive look at Sony's hacking saga. *Vanity Fair*. Retrieved from http://www.vanityfair.com/hollywood/2015/02/sony-hacking-seth-rogen-evan-goldberg

Shearlaw, M. (2016, January 25). Egypt five years on: was it ever a 'social media revolution'?. *The Guardian*. Retrieved from http://www.theguardian.com/world/2016/jan/25/egypt-5-years-on-was-it-ever-a-social-media-revolution

Shieber, J. (2014, March 12). Goldman Sachs: Bitcoin is not a currency. *Tech Crunch*. Retrieved from https://techcrunch.com/2014/03/12/goldman-sachs-bitcoin-is-not-a-currency/

Shwartz, M. J. (2014, March 17). DDoS attacks hit NATO, Ukrainian media outlets. *Dark Reading*. Retrieved from http://www.darkreading.com/attacks-and-breaches/ddos-attacks-hit-nato-ukrainian-media-outlets/d/d-id/1127742

Slater, D. (2002). Social relationships and identity online and offline. In L. Lievrouw & S. Livingstone (Eds.), *Handbook of new media: social shaping and consequences of ICTs* (pp. 553-546). London, U.K.: Sage Publications.

Slaughter, A. M. (1997). The real new world order. *Foreign Affairs*, *76* (5). Retrieved from https://www.foreignaffairs.com/articles/1997-09-01/real-new-world-order

State of California Department of Justice Office of the Attorney General. (2014, December 8). *Sony Pictures Entertainment notice letter*. Retrieved from https://oag.ca.gov/ecrime/databreach/reports/sb24-47706

Steinberger, H. (1981). *The encyclopedia of international law*. Amsterdam: North-Holland Publishing Co.

Sterling, B. (1992). *The hacker crackdown: Law and disorder on the electronic frontier*. New York: Bantam Books.

Student Daily News. (2010, December 15). Stuxnet virus set back Iran's nuclear program by 2 years. *Student Daily News*. Retrieved from http://www.studentnewsdaily.com/daily-news-article/stuxnet-virus-set-back-irans-nuclear-program-by-2-years/

Tanenbaum, A. S. (1996). *Computer networks*. Upper Saddle River, NJ: Prentice Hall.

Tatar, Ü. (2015). RedHack: A Hacktivism case study. In L. Jarvis, S. MacDonald & T. M. Chen (Eds.), *Terrorism online: politics, law and technology* (pp. 54-71). New York: Routledge.

Taylor, C. R. (1997). A modest proposal: Statehood and sovereignty in a global age. *University of Pennsylvania Journal of International Economic Law, 18*(3), 745-809.

Technopedia. (2016). 'computer network' definition. Retrieved from https://www.techopedia.com/definition/25597/computer-network

Templeton, G. (2014, August 4). Snowden went too far by revealing the NSA's MonsterMind cyber weapon. *ExtremeTech.* Retrieved from http://www.extremetech.com/extreme/187992-snowden-went-too-far-by-revealing-the-nsas-monstermind-cyber-weapon

Tiezzi, S. (2015, June 24). China's sovereign Internet. *The Diplomat.* Retrieved from http://thediplomat.com/2014/06/chinas-sovereign-internet/

Trachtman, J. P. (1994). Reflections on the nature of the state: sovereignty, power and responsibility. *Canada - U.S. Law Journal, 20*(39), 399-415.

Trachtman, J. P. (1998). Cyberspace, sovereignty, jurisdiction, and modernism. *Indiana Journal of Global Legal Studies*, *5*(2), 561-581.

UkrTelecom Statement. (2014, February 28). *Ukrtelecom's Crimean sub-branches officially report that unknown people have seized several telecommunications nodes in the Crimea*. Retrieved from http://en.ukrtelecom.ua/about/news?id=120467

UN Charter. (1945). *Charter of the United Nations and Statute of the International Court of Justice.* Retrieved from http://www.un.org/en/charter-united-nations/

US Department of Homeland Security. (2003, February). *National strategy to secure cyberspace*. Retrieved from http://www.dhs.gov/national-strategy-secure-cyberspace

Vanderbilt University. (1996). *Postmodernism and the culture of cyberspace* [Fall 1996 course syllabus]. Retrieved from http://www.vanderbilt.edu/AnS/english/Clayton/sch295.htm

Weber, M. (1946). *From Max Weber:* E*ssays in sociology.* New York: Oxford University Press.

W3Techs. (n.d.). *Usage of content languages for websites*. Retrieved from https://w3techs.com/technologies/overview/content_language/all

Weinberger, D. (2002). *Small pieces loosely joined: A unified theory of the Web*. Cambridge, MA: Perseus.

White House Office of the Press Secretary for Immediate Release. (2015, January 2). *Executive order imposing additional sanctions with respect to North Korea*. Retrieved from https://www.scribd.com/doc/251531426/North-Korea-Sanction

Williams, C. (2012, June 1). Barack Obama ordered Stuxnet cyber attack on Iran. *The Telegraph*. Retrieved from http://www.telegraph.co.uk/technology/news/9305704/Barack-Obama-ordered-Stuxnet-cyber-attack-on-Iran.html

Wiseman, P. (2008). Cracking the 'Great Firewall' of China's Web censorship. *ABC News*. Retrieved from http://abcnews.go.com/Technology/story?id=4707107&page=1

Wong, G. (2015, December 16). China touts its great firewall in push for Internet control. *The Wall Street Journal*. Retrieved from http://www.wsj.com/articles/china-touts-its-great-firewall-in-push-for-internet-control-1450251090

Wriston, W. B. (1997). Bits, bytes, and diplomacy. *Foreign Affairs*, *76* (5), 172-182.

Xuecun, M. (201, August 17). Scaling China's Great Firewall. *The New York Times*. Retrieved from http://www.nytimes.com/2015/08/18/opinion/murong-xuecun-scaling-chinas-great-firewall.html?_r=0

Yin, R. K. (1993). *Applications of case study research.* Newbury Park, CA: SAGE Publications.