GOVERNING TURKEY'S INTERNET:

CYBER SECURITY AS A STRATEGY OF POWER

DENİZ ZERİN

BOĞAZİÇİ UNIVERSITY

2016

GOVERNING TURKEY'S INTERNET:
CYBER SECURITY AS A STRATEGY OF POWER

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
Sociology

by
Deniz Zerin

Boğaziçi University
2016

DECLARATION OF ORIGINALITY

I, Deniz Zerin, 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 ....8/8/2016........................

ABSTRACT

Governing Turkey's Internet:

Cyber Security as a Strategy of Power

This study investigates expansion of the field of cyber security in relation to governing of the Internet in Turkey within the last decade. It argues that security rationality is becoming the dominant diagram in evaluating problems and solutions associated with the Internet. It shows that cyber security is instrumental in expansion of forms of power associated with security objective through a discourse of risk and danger, institutional restructuring, law making, and most importantly, technical practices. Technical practices, for they have a indirect relation with the infrastructure of internet communications, represents a reflexive quality, which makes cyber security field element of a distinct strategy of power, in the intersection of government, technology and security.

ÖZET

Türkiye'de İnternetin Yönetimi:

Bir İktidar Stratejisi Olarak Siber Güvenlik

Bu tez Türkiye'de internetin yönetilişinde siber güvenlik alanının etkilerini incelemektedir. Savı Türkiye'de son on yılda İnternet'in yönetilişinde güvenlik zihniyetinin ağırlık kazandığı, ve siber güvenlik alanının bu olguya katkıda bulunduğudur. Siber güvenlik, ilgili olduğu risk söylemleri, kurumsal yapılandırma ve yasama ve teknik pratikler yordamı ile İnternet'in güvenlikli̇leştirilmesine katkıda bulunmuştur. Tez güvenlik stratejilerinin etkinliğinin artışında iki tarihsel an tanımlayıp, siber güvenlik alanının genişlemeye başladığı 2011 yılından itibaren, internetin yönetiminin teknik sorunlarla ilgilenmeye ve teknik bir dil edindiğini söylemektedir. Siber güvenlik pratikleri, internet iletişiminin altyapısı ile dolaysız bir ilişki kurdukları için, dönüşlü (refleksif) bir nitelik taşır. Bu siber güvenliğe bir iktidar stratejisi olarak yönetme, teknoloji ve güvenlik kavramlarının etkileşiminde olmasından kaynaklı özgün bir nitelik kazandırır.

To my loving family, without whose support this thesis would not have been finished.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

This thesis seeks to illustrate the ways in which cyber security has become a dominant political issue in recent years in Turkey. Protection of digitalized information is a major political problem, one that which stands out among other kinds of problems that include telecommunications technology and the Internet. As I argue in this thesis, cyber security is becoming a dominant framework in which internet technologies are evaluated, designed, structured and used. Cyber security puts forward a political rationality, in which security priorities and anxieties dominate all other ways of making sense of political problems that which Internet causes. Once seen as an opportunity for catching up with the ¨global information society[1] and economic development, the Internet is being increasingly portrayed as a space of danger and risk that threatens anyone and everyone.

While cyber security practices and rationality is gaining the upper hand in the government of internet technology, internet users in Turkey are less safe than ever. Giant data leaks of personal information take place; police forces take users in custody for expressing their views on social networks; and cyber-attacks bring down the whole local domain network with ¨com.tr¨ websites. In addition, there is extensive online censorship of online newspapers, educational websites, activists' networks, and of dissident social media accounts. Attempts to decentralize internet infrastructure have come to an end since smaller internet service provider companies were left unable to renew their

[1] The term 'information society' is often used to stress the increasing role of information and its liberating potential in shaping economy, culture and politics (Castells, 2002). While proponents of information age in the field ascribe a positive character to it, increasing cyber security concerns, and proponents of those concerns stand at odds with such attribution.

licenses and eventually TTNET has now become the monopoly service provider. Laws are passed to oblige service providers to collect traffic data of their users, which makes surveillance easier, while placing users at risk for the protection of personal data. State institutions that are especially responsible of security, surveillance and control have the utmost authority in shaping the internet access. Clearly the Internet is no longer seen as a ¨information superhighway[2]¨ that can benefit all, but rather as a menace that needs to be tamed.

In order to make sense of the greater changes in the governing of the Internet in Turkey in recent period, I use cyber security practices and the political rationality they represent as an entry point. I argue that cyber security has provided strategic tools for the governing[3] of the Internet, so that rationality of security becomes the dominant element. This process has been largely shaped by the discourse of threats, legislation that shapes cyber security conduct, institutional formation and restructuring, economic incentives to encourage security work among software engineers and NGOs' presence as major actors. Neoliberal political rationality is at work in internet governance, however the role of cyber security practices function in ways more intricate than theories of neoliberal political rationality can explain. There are elements unique to strategies of power affiliated with security rationality and ¨technological society[4]¨.

[2] Information superhighway is a term used for defining the Internet, mostly used in the 1990's in the United States. The term reflects the political conviction of the period that stressed the autonomy of Internet, which was based on the shared understanding of the Internet as fundamentally decentralized entity, therefore impenetrable by outside forces. Chapter 2 includes a discussion on this topic.

[3] Throughout the thesis ¨governing¨ and ¨government¨ are used interchangeably. A similar concept, ¨governance¨ is also used, particularly when stressing relations between actors of governing. Governing or government is used to denote the overall social and political process.

[4] Andrew Barry (2001, p. 2) explains technological societies as ¨one which takes technical change to be the model for political invention¨.

The research that this thesis is based on is motivated by the influx of news stories about cyber warfare and cyber security that were in circulation in the first half of 2013. As a term, cyber warfare was a relatively unknown to general public at the time, although its popularity was increasing among international relations and military experts, due to discovery of Stuxnet cyber sabotage virus. In 2010, Stuxnet leaked into the uranium enrichment facility in Iran, damaging uranium enrichment process, crucial for nuclear power plants and atomic weapons. Iranian officials have identified the source of the damage in December 2012, and declared that it was an act of sabotage with the aim of bringing uranium enrichment process to a halt.[5] The event caused diplomatic distress between Iran, USA and Israel. In this period of diplomatic tension, analysts wrote articles explaining terms such as cyber security and cyber warfare, increasing the visibility of expert knowledge about cyber security in the media. With the Internet, nuclear reactors, software viruses and sabotage brought together in a spy-movie-like story, cyber security became a hot topic.

In a broader perspective cyber security anxieties can also be linked to whistleblower activities. In 2010 Wikileaks have published several files, all of which include classified correspondence among diplomatic personnel of the United States government. The leaks of these correspondences have had detrimental effects on the United States' foreign policy at the time.[6] For the Turkish officials, anxiety of similar kind of leaks became apparent, especially after the dissident hacking collective Redhack published classified information. Redhack leaked numerous documents and archives, most prominent being documents that prove gendarmerie intelligence department had

[5] (Nakashima & Warrick, 2012)
[6] (Leigh, 2010)

previous intelligence about preparations being made for the Reyhanlı bomb attack, yet did not act on it[7].

As the foreign news bureaus of major world newspapers were busy keeping up with the diplomatic tension, local reporters were digging into Turkish states cyber warfare capability and apparent problems. A simple research about the current situation of cyber security practices in Turkey at the time revealed that, those who are engaged in digital systems security have been using concepts and discourses of militarism for some time, as exemplified in conference presentations made by Cyber Security Foundation (Siber Güvenlik Derneği) affiliated researchers.[8] Security Conference 2012 had a sloppy looking website, explaining the conduct of cyber warfare, treating information infrastructures as battlefields and revising technical jargon with militaristic jargon.[9]

1.1 Why study cyber security?

Cyber security requires research for various reasons. Firstly, it is a newly forming field. As we already hinted briefly, especially in Turkey, the implementation of practices of cyber security has gained momentum. In less than a decade, cyber security became one of the major topics of debate within telecommunication technology circles. It is possible to see the haste in which laws regulating cyber conduct of state institutions, private companies and individuals have been passed. With legal documents of varying function

[7] Even though cyber security initiatives predate the period in which Redhack made publicized hackings and leaks, Redhack's actions has contributed to security anxieties that motivated the development of cyber security practices. (Hürriyet, 2012)

[8] Bâkır Emre's presentation "Offensive Approaches to Cyber security" in Cyber Security Conference 2012 stands out as an example. (Emre, 2012a)

[9] (Emre, 2012b)

and quality, it is possible to talk about a surge in practices of cyber security. This fact alone, reveals the need for a sociological research on the topic of cyber security.

The momentum in which cyber security measures have been put up is visible in various locales. It is important to mention some of these, just to give an idea about the scope of cyber security practices and their effects on society on a greater level.

It is possible to talk about a surge in computer engineering circles, with articles published, workshops and discussion panels organized that take cyber security as its focus. There is an increase in diffusion of expert knowledge. On a global level, research funds are increasingly available for cyber security experts.[10] Turkey is trying to catch up with this trend, by participating in EU programs, which fund cyber security research. Despite their efforts, Turkish cyber security experts mostly follow foreign research, rooted in USA and Israel. There is limited research for producing knowledge about cyber security. Instead the focus is on distribution of expert knowledge imported from said countries on cyber security, through seminars and workshops.[11] There appears to be demand for cyber security experts and the protection they provide. Agents of commerce especially seek for expert services, and this fact resulted in digital systems security becoming a preferable career option for newly graduated computer engineers. As many computer engineers are starting their careers in security firms, technical expertise about telecommunications technologies get to be dominated by security discussions and security professionals.

[10] US National Science Foundation has granted 74 million dollars for interdisciplinary cyber security research (National Science Foundation, 2015). Additionally, there are funding efforts by European Development Agency, in which TUBİTAK collaborates (AB Hibeleri, 2016).

[11] The case of the national operation system PARDUS is an example of how cyber security research is limited. As I explain in depth in chapter 3, state sponsored PARDUS project was shut down, resulting in the dissipation of expert knowledge in open source software and software security that has been produced by PARDUS team.

As the field of cyber security is newly forming, there are efforts to define the field by those who are part of it. There are online newspapers focusing on cyber security, as well as blogs and video channels[12]. However, these are limited in comparison with the growth the field is experiencing. The approach of cyber security experts in defining their expertise is rooted on a strongly perceived technical necessity. The function of cyber security, thus, is often formulated as following a necessity that has to be fulfilled. These definitions appear to take cyber security simply as a technical issue, which this thesis aims to challenge, by introducing a sociological framework. A lack of cyber security experts to generate comprehensive understanding of their practices is one of the major reasons this thesis has been written.

1.2 Motivation for studying cyber security

Initially, the way cyber security practices became apparent in the media was linked to the needs of private companies, particularly the banking sector, and the state institutions. Companies demand protection for data that are stored in their own digital systems. With Redhack leaks becoming publicized, the same kind of demand arose from the state institutions. Thus third party access into business or state data, held digitally, was a major fear. While information security became visible under the cyber warfare heading, those who work in telecommunications NGOs have been pushing Ministry of Transportation, Maritime Affairs and Communication for the passing of legislation

[12] Online news portal www.siberbulten.com , which compiles news about national and international developments is one of its kind. Avery good blog featuring debate on anonymity and critique of security measures is https://network23.org/kame/ .

setting the framework for citizens' individual data security. The law was passed in March 2016, during the last stages of this research.[13]

In this sense, cyber security seems to be not about protection of the personal information, but rather protection of digital systems that store information. The focus of practices and technical tools of cyber security is securing digital systems, a focus, which does not directly deal with personal information. Cyber security deals with the technical infrastructures. Development of new technologies and security rationality has been hand in hand throughout history. Many technological inventions have come up to satisfy the needs of military, and this was particularly the case for telecommunications technologies[14]. This is precisely how cyber security brings telecommunication technologies and practices and strategies of security together. However, it facilitates this not in the traditional way that uses communications as an element of security/warfare, but rather as an element of security of communications.

There is something peculiar about cyber security in general. Cyber security is about protection of telecommunications infrastructure. In a sense, it is a form of technology that primarily aims to protect technology. As my research went on, I found an interesting level of reflexivity within the core of cyber security practices and strategies. Cyber security practices rely on software that seeks to protect software. Cyber

[13] (Anadolu Ajansı, 2016) Law Regarding Protection of Individual Data, has been passed following several interventions into the initial draft proposed by civil society organizations. Law states that in order for institutions to process personal information, there should be 'open consent'. However, law does not define what constitutes open consent. An earlier draft where consent was defined as a written document has been left out in the final version. Additionally, law allows for processing of sensitive information, such as ethnic, religious or political information, under the conditions where undefined precautions by "board of data protection" has been executed (Nebil, 2016).

[14] Andrew Barry explains the electrical telecommunications as the "ultimate liberal military technology, an invisible deterrent" (Barry, 1996).

security belongs to the ensemble of internet technologies which seek to conserve the functioning of the internet as it is.

My main motivation in studying cyber security rests in this reflexivity. I was interested in how reflexive technologies can have security objectives. Instead of applying and adjusting technological tools and practices to the conditions of security crisis, I wanted to study how security rationality can be incorporated in technological governing practices. I was tempted to think how the protection of technology must be different from using technology to protect something external to technology. Study of the processes in which telecommunications technology deals with problems arises from within itself, and calls for an approach that takes its relative autonomy into account. As this thesis focuses on the government of the internet, it allows for studying the kinds of implications reflexivity has on the governing of internet and the role cyber security plays in governing in general. Reflexivity of cyber security causes practices of cyber security to depend on the technical. If technical aspects of security are prominent, rather than, say, moralistic aspects, this is due to the reflexive nature of cyber security.

Studying cyber security is crucial particularly because there seems to be a continuous neglect of discussing the social aspects of digital systems in government circles. Cyber security seeks to conserve the status of the digital systems in question, and most of the techniques it relies focuses on conserving, rather than liberty or transparency. Even though necessity for protection of digital systems may have a solid base, there appears to be little discourse and logic to direct security efforts towards aligning them compatible with collective and individual freedom.

Society enters in the analyses of cyber security experts as a source of problem and malfunction, in a subordinate position to the requirements of the technical. Therefore this thesis situates cyber security and its technical requirements within greater societal forces, rather then vice versa, and studies the impact of cyber security measures on the way in which internet technology finds uses and a shape in society.

A study of cyber security practices through the lens of social sciences can help generate a societal framework within the actors of government of the Internet. I think cyber security can take a form that expresses the security needs of individuals and collectives. However the current way in which cyber security policymaking operates neglects social needs, including the protection of personal information and freedom of encryption and anonymity. Cyber security policymaking is centered on the needs of the large businesses and state institutions. The economic interests of businesses and the political interests of governments dominate the current cyber security policymaking. If there is ever to appear a socially conscious cyber security policy, it should be conscious about its impact on society as a whole. This is the reason the thesis puts governmentality framework[15] to use, in hopes that such a framework can provide a conceptual background for cyber security policies effects on the internet use in Turkey as a whole.

This thesis links apparatuses of control with policies of cyber security. If governing circles keep on neglecting social needs for cyber security, which appears to be most likely, resistance to such policies will require a linking of cyber security practices with broader mechanisms of control that are in effect in internet governance. Current internet activism in Turkey focuses mostly on censorship and surveillance. While

[15] Second chapter features a comprehensive explanation of the concept of governmentality and the theoretical framework that the concept is based on.

censorship and surveillance are urgent issues, that rightly draw activists' efforts, an overview of cyber security technologies will provide such efforts tools that can be used to generate a broader understanding of internet government in Turkey.

That is because some of the technical tools employed in cyber security practices are also used in nation wide surveillance. Effective national cyber security practices require information about internet users; their online habits, their technical capacity and contents of their traffic. Technical tools used to peek into traffic of internet users, on individual and collective level are present. Among these, namely the services provided by Phorm, are used to inspect the contents of individual and nationwide traffic[16]. Inspection of the content of traffic is necessary, for example, for the evaluation of DDOS attacks originating from computers in Turkish network. A company of similar kind that sells digital surveillance and censorship tools is Netclean. Netclean products are also an elementary feature of URL-based censorship[17].

All in all, surveillance, censorship and cyber security appear to be mutually constitutive parts of a bigger whole, and that these practices have a complex relationship with each other. So when we criticize the ineffectiveness of state institutions in protecting "com.tr" signed websites from cyber threats, and do not criticize the current understanding of cyber security policy, we could be calling for more authoritarian technological tools that can result in stronger surveillance.

[16] (Kuzuloğlu, 2012)
[17] (Kus, 2014)

1.3 Research questions

The main interest of this thesis is the processes in which elements of society shape technology and vice versa. The domain of Security, as an element of existing social forces, is capable of shaping the development of communications technology. Institutions and individuals that rely on a discourse of security have technical capacities that enable them to contribute to development of the Internet related technologies. While investment into solutions towards security anxieties have an extended ground in current societies, do anxieties and solutions of security diverge from one another in different domains of social life? This thesis argues that practices of security in the case of internet governance is distinct from domains of social life unrelated to technology and telecommunication. Even though expansion of cyber security institutions and practices are located in the general expansion of society wide security anxieties, it is based on technical requirements of internet infrastructure. It is this technical aspect in defining security problems and solutions; cyber security becomes distinct. It comes to embody a strategy of power distinct from other domains in which security rationality takes hold.

I think it is crucial to note that security rationality does not only use technology as a tool, it sometimes takes technology as its objective. Cyber security protects telecommunications technologies from dangers that are by products of telecommunications technologies themselves. Subject matter of protection is of digital systems, dangers being malfunction or outsiders who wish to infiltrate into information systems.

This thesis relies on three fundamental issues: security, technology, and governance/government. And it sets out to find explanations for particularly one general question: How do security rationality and security practices, embodied in cyber security practices, affect internet technologies and the ways in which these technologies are shaped/governed? More particularly these are the questions that were present in the writing of this thesis:

- What are some main objectives of internet governance in Turkey?
- How is it possible to make sense of security discourses and practices that are effective in internet governance circles in Turkey?
- How does security rationality affect governing processes?
- In what ways do cyber security measures reflect security rationality?
- In what ways do cyber security measures effect the governing of internet in Turkey?
- How does cyber security differs from morally grounded discourse and practices of security?
- Which actors have gained an upper hand, and which actors have lost influence as a result of the increasing security-oriented practices?

1.4 Methodology

Data that this thesis relies on is derived through mixed methods: a reading of primary and secondary sources as well as fieldwork.

1.4.1 Primary and secondary sources

In acquiring a greater understanding of cyber security practices, I relied on primary sources. News features from newspapers, weeklies and magazines were crucial for the research period of this study, for they allowed me to gain information about law-making process, institutional practices, and meetings between actors of governance. As almost all security work, cyber security work requires a level of secrecy, which makes it difficult for outsiders to gain information. Especially when the institutions in question are state institutions.

Research about cyber security practices necessarily involves state institutions. As the theoretical framework of this thesis located cyber security practices within a totality of governmental practices related to the Internet, state institutions that take part in governing of the Internet were at the focus of my research. Of these institutions, such as semi state-owned internet service provider TTNET and Communication Technologies Authority (BTK) stood out. I did not (and could not) investigate the inner workings of these two institutions. Instead, I located their primary functions in a study of government processes. Data about these institutions were acquired from either news articles or the publications of these institutions.

Aside from TTNET and BTK, certain other state institutions were particularly important in the cyber security circles. The Telecommunications Authority (TİB) can be mentioned as the primary institution, even though it is not directly linked to execution of cyber security practices. However, TİB is the main actor that views the Internet as a security problem, and acts according to a security logic. As the institution that is responsible of executing wire tapings, court ordered digital surveillance, website censorships and initiating filters to internet traffic, TİB is the main driving force, I argue, of the move towards security orientation in internet governance circles. TİB has an advanced Q&A section in their website, clearly describing their legally defined duties. I have made use of these documents. TİB's website also hosts a section for inquiry for information, though I did not make use of it.

1.4.2 Fieldwork

Fieldwork that this thesis relies on has focused mainly on the NGO's that serve in the cyber security field. I participated in the public events, namely Cyber Security Conference '13 & '14 and 6th International Conference on Information Security & Cryptology, that cyber security NGO's Cyber Security Foundation (Siber Güvenlik Derneği) and İnformation Security Foundation (Bilgi Güvenliği Derneği) organized. I participated in an information security workshop within 6th International Conference on Information Security & Cryptology. Participant speakers of the workshop and conferences organized by these NGOs included high profile bureaucrats and experts from the private sector. These events were particularly fruitful for they allowed me to witness the relations among experts from telecommunications and banking companies, NGOs executives and state telecommunications bureaucrats.

I briefly participated in the public events that open source community in Istanbul has organized. One of these events, Free Software and Linux Days '13 organized by Bilgi University, included a panel in which experts from TUBİTAK have set out to inform the public about their latest open-source operating system. As it turns out, the operating system, PARDUS, was mostly, according to the open source community members, a copy of the existing operating release that have been published previously. It was a crucial part of the fieldwork I conducted, for it allowed me to witness the tension between open source software developers and state officials, and the difference of degree of expertise they posses. As it became apparent that open source community members were much more dedicated and motivated and held greater technical information, some of the cyber security strategies, such as ¨increasing awareness¨ made much more sense. Because, the so to say ¨dissident experts¨ have been on a different technical capability level, and cyber security strategy that the state institutions employed, appeared to be geared against these dissident experts.

Additionally, I interviewed the owner Atilla Aydınalp and the workers of Pan Yazılım, a software development company that produces the firewalls/filtering software that the law requires internet café owners to install in their computers. As a low-profile cyber security job, the production of filtering software is supported by state telecommunications agencies. Of the filtering software producing companies I have interviewed a relatively smaller one. These interviews allowed me to witness the point of view of the software engineers that have aligned with the cyber security policies that are upheld by state institutions. As the macro-level experts view cyber security as a national security matter or commercial risk prevention job, software engineers who are at the bottom in terms of effecting the direction of cyber security governance view their labor as a means to provide income. Cyber security governance has shaped lives of many software engineers as it has created jobs through state support and incentives.

1.5 Organization of the study

The multiplicities of the locales where I have conducted fieldwork have encouraged me to frame cyber security as an element in a greater whole. Rather than conducting an in-depth study of cyber security practices in Turkey, this thesis locates cyber security practices, as kinds of practices that effects the way in which internet technologies are shaped in Turkey. It is a study of cyber security practices, primarily from the standpoint of government of internet technologies.

The field in which cyber security practices are a part of appears to be contingent and ever changing. As the field of cyber security is currently being established, and the fact that cyber security is becoming a major issue today is a sign of changing forces that shape the internet experience of users and distribution of information, I decided to employ a framework that can allow me to see cyber security practices as part of a process.

I relied mostly on governmentality literature. Governmentality offers a useful framework for understanding the shaping of our political present, without course to dualisms or reductions. As Michel Foucault's concept of governmentality deals with macro level changes in society, namely the art of government taking the population as its main object, I made use of works by scholars belonging to Anglo-Foucauldian tradition. I rely on the works of Andrew Barry, and the idea that telecommunications technologies not only shape the government of society in general, but they shape what we see as political problems and solutions.

This thesis deals with the cyber security field, including practices, institutional formation, legal documents and NGO's. It seeks to identify technologies of power that can be attributed to components within the field. Concerns about security provide a wide range of actions and strategies for power to effect and shape reality, especially when it is coupled with a governing rationality. Michel Foucault's discussion of the "security apparatus" is essential to this thesis. While Foucault's discussion of security takes population as its object, I applied his ideas to a technological field, the governance of the Internet.

The thesis is structured into three chapters. Chapter 2 sets the theoretical framework. Chapter 3 puts forward the uses and effects of cyber security practices. Chapter 4 explains the current condition and main elements of internet governance in Turkey.

Chapter 2 sets the framework in which internet technology and cyber security measures are discussed in this thesis. It provides a very brief outline of Michel Foucault's genealogy of power. Foucault's use of the concept of power is peculiar and is of central importance for the extensive explanation of the concept of governmentality, on which this thesis is based on. Thesis relies on conceptualizations brought about by theorists of Anglo Neo-Foucauldian School. As theorists such as Colin Gordon, Mitchell Dean, Nicolas Rose and Andrew Barry, of said school seek to use Foucault's concepts as a base for exploring political rationalities, their works have been particularly crucial in pointing out the links between governing and the political process in which cyber security practices are a part of.

The works of Andrew Barry have been particularly crucial in my work. As Barry's work has focused on uses of technology in governing and making of societies, many of the theoretical links between internet governance and politics are founded on his work. Chapter 2 additionally aims to provide some of the theoretical discussions from the sociology of technology field. Question of technological determinism is a central point of debate among sociologists and historians of technology. An extension of this debate is the problem of autonomy. Researchers employing the institutional economics standpoint write extensively on the issue of autonomy of internet infrastructure, so there is a section about their works as well. Finally, there is a brief account of the academic works about internet governance in Turkey.

Chapter 3 discusses the main research findings of the thesis. Chapter begins with definition of cyber crime and its relation to cyber war. Section on the legal basis of cyber crimes includes an overview of the laws and policy documents that are used. National and international documents occupy a crucial role in the making of cyber security policy. In global debate on models of internet governance, cyber security occupies a unique role. Actors who value security above other elements of governance insist on problems that lack of cyber security poses, and use their point to push forward a more centralized governance model. Formation of the cyber crimes police has a crucial role in the functioning of cyber crimes practices. This function is explained in the brief history of the making of the cyber crimes police forces.

Lastly, Chapter 4 introduces some of the main actors in internet governance field in Turkey. Chapter begins with an overview of internet infrastructure and the role of monopoly internet service provider company TTNET. Laws and legal documents that are central to the main problems of internet governance in Turkey is introduced in the second subsection of this chapter. One of the most important actors of the internet governance in Turkey is the Telecommunications Authority (Telekomünikasyon İletişim Başkanlığı - TİB). The role that TİB plays in internet governance is based mainly on censorship and surveillance practices. The technical process in which censorship happens is explained in brief. Some of the recent institutional arrangements that were made for organizing censorship practices are explained under the heading of Access

Providers Association (Erişim Sağlayıcıları Birliği). Additionally some private companies, such as Phorm, and technical tools, such as Blue Coat are introduced in this chapter. The governing of computer engineers and their expert knowledge is crucial in understanding the current state of the Internet in Turkey. Because of that, a subsection is devoted to the general policy regarding the computer engineers and among those who become cyber security experts. Finally, there is a very brief account of how organized resistance to current internet governance in Turkey takes shape and the main problems they deal with.

CHAPTER 2

THEORETICAL ASPECTS: FROM CONTROL TO GOVERNMENT

Before we examine the current condition of internet governance in Turkey, a presentation of analytical tools that are suitable for such an examination is necessary. This section will provide a brief outline of main debates within the field technology of sociology and an outline of various formulations of concept of governance/government, particularly with respect to digital technologies. Such an outline will hopefully show various conceptions offered regarding the role of technology in power relations. As the thesis uses the concept of ¨government¨ to approach its subject matter, an introduction of the concept of government will follow.

In order to develop the theoretical background of this study, this section includes three subsections that focus on distinct theoretical fields. The first subsection focuses on historical-sociological theories of technology. The second subsection focuses on the concept of government and the theory of governmentality. The third subsection provides an outline of the scholarly studies conducted in Turkey, on issues outlined in the first two subsections.

The first subsection starts with an account of technological determinism debate. ¨Technological determinism of society¨ vs. ¨social construction of technology¨ was a debate in the 1980's among historians and sociologists of technology. Technological determinism was critiqued for its reductionist conception of the role of technology in society, while the other, though prominent side of the debate, critiqued for excluding the technology's effect on society altogether. [18] By focusing on the criticisms of ¨technology determining the individual psyche¨ approach, the subsection examines the deterministic approach to relationship between technology and power relations. Similar points of debate are presented in this first subsection, particularly the role of technological determinism in the historical materialist conceptions of development of capitalism.[19] The overview is then extended to techno-libertarians who wrote in the early days of the Internet. While they see an autonomous space in the Internet, some others see a darker picture.

The second subsection begins with a specific use of the concept of government. Scholarly field of institutional economics sees in concept of government institutions and their internal workings. Institutional economics focuses on corporate, NGO and state actors, which renders representation of constituents within governing institutions as the primary problem of government. From there on, Michel Foucault's conception of governmentality is introduced, a concept which scholars rely heavily in studies of critical government. In this line of thought, Andrew Barry's work on government of technological societies[20] is particularly important. Barry provides important insights as to how technology shapes our understanding of the political.

[18] For a historicized account of the debate see: (Allen & Hecht, 2001). Also see: (Winner, 1993).

[19] Whether Karl Marx's ideas on the role of technology carry technological determinism is a matter of debate. Marx provides a grounded discussion on the role of technology in society, through an analysis on the role of technological innovation in production process and reproduction of class divisions. Marx's conception, in addition with Marxists critiques that provide information technologies a relative autonomy, are crucial in understanding both positions taken in the technological determinism debate.

[20] Andrew Barry refers to technological society as a form of order in which technological problems are central to political preoccupations. In technological societies ¨technical change is the model for political invention.¨ In technological societies interactive and networked devices are ¨thought to provide a significant part of the solution to the problem of forming the kind of person who can exist, manage, compete, experiment, discover, invent and make choices¨ (Barry, 2001, p. 31).

The third subsection presents an overview of scholarly works of academics studying internet use and internet government in Turkey. Topics of research vary from researcher. While some focus on the statistical aspects of internet literacy and use in Turkey, others take educational potential of internet as the focus of their work. Furthermore, the Internet is studied in relation to addiction, in relation to risks and activism. Özgün Topak's study of internet governance and Burçe Çelik study of politics of techoscape in relation to dissident politics have guided this study, in terms of field research and theoretical framework employed.

2.1 Selective review of scholarly discussions on the Internet

Academic discussions regarding the nature and the application of the Internet was not lacking since the first days of its development. Academics, technologists, computer scientists and sociologists wrote extensively about the Internet. Developments it made possible became subject matters of wide discussion, with remarks on the 'nature' of the Internet with pretenses such as progressive or dangerous. An extension of a continuing debate on the nature of technology, some argued that the Internet is the locomotive for human advancement. And human advancement can be attained with the help of the Internet because; it is potentially a space in which freedom can be organized. As the early studies about the Internet argued heavily, Internet defied limitations posed by states, for the Internet is fundamentally de-centered (Barlow, 1996). On the other hand, there were many who saw in Internet a capacity for a different kind of enslavement, in which technology could enable an authoritarian rule (Morozov, 2011).

Early technologists believed in the idea that Internet can be used for the better. They believed that the contributions that Internet could make for the betterment of the human condition results from the Internet's design (Barlow, 1996). These arguments highlighted that the technological problems regarding architecture of the internet are political in character.

2.1.1 Technological determinism

The duality of 'inherently harmful Internet' and 'inherently progressive Internet' rely on a theoretical debate that has been central in sociology of technology. It is the question of technological determinism that makes arguments of this kind possible.

Technological determinism is a theoretical approach in which sociological problems are addressed with technology given a determinant position. It takes technological systems or technological artifacts as its starting point for sociological analysis. Technological determinist approach argues that technology shapes social relations, not the other way around. Consequently, technology has a grander standing in hierarchy of causality. Technological deterministic arguments concerning Internet portray the relationship between the Internet and humans as one sided, in which humans are inactive agents. Technological determinism is often critiqued, and when used as a label, it usually has negative connotations.

Among the theoretical positions that critiques of technological determinism are geared towards are: Medium Theory and Marxist Theory (Cavanaugh, 2007).

For theoreticians of Medium Theory[21], technology acquires its deterministic quality from its capacity to organize human perception. Media has capacity to extend human perception of time and space, of which have different consequences on human organization. Medium Theory argues that ¨Technologies organize, select and focus environment through various transformational structures¨ (Ihde, 1979, as cited in Cavanaugh, 2007). Harold Innis argues that information preservation technologies that can only preserve information for only short periods of time, as in traditional societies; and that which is regarded as truth extends over time. As the truths are taken over by next generations, these societies tend to be conservative (Innis, 1986). In the same vein, Marshall McLuhan argues that medium, brings about the message, which is ¨change of scale, or pace, or pattern that a new invention or innovation introduced into human affairs¨ (McLuhan, 1964, p. 8).

Aside from determinism of human faculties, there is a strand of technological determinism that focuses on the constitution of material relations in society. Writings of Karl Marx are argued to be in this strand (Winner, 1978). Although there are conflicting accounts as to how did Marx view technology in his critique of capitalism, his methodology is crucial for the sociologists of technology regardless. Marx's critique of political economy represents a scientific approach to laying the structural elements that creates and sustains power relations in society. His framework allows students of sociology of technology to locate the role production, circulation and consumption of

[21] Medium Theory is an approach within the Communications and Media Studies, that states medium, instead of content, shapes the way humans create meanings and values. Medium theory argues that medium, as symbolic environment of a media, ensembles social and political order in which certain content can be transmitted while others cannot. Scholars focus on types of medium, and differences among them, and the way each effect material, psychological and social processes. Marshall McLuhan and Harold Innis are among the leading scholars of Medium Theory. For primary texts see: (McLuhan & Fiore, 1967) and (Innis, 1986).

technologies. For this reason in order to locate internet technology in broader social relations an analysis of Marx's though is required.

The degree Marx attributed a causal role to technology remains an object of debate. These debates revolve around Marx's conception of mode of production. While, critics of Marx see in his writings a one-way relationship between technological advancements in the production and the relations of production; stressing the circular role of production and social relations often refutes these criticisms.

As Etienne Balibar explains (Althusser & Balibar, 1970) in Marx's thought, the concept of mode of production serves as the main framework in which the totality of social relations ensemble into a coherent picture. In categorizing the totality of the 'social', the concept of mode of production involves forces of production that is the material conditions and artifacts. The conditions and artifacts serve as the condition of possibility of a mode of production, as well as create conditions for the reproduction of current relations. In addition, the mode of production includes relations of production, that is class division of society that arises out ownership of means of production. According to Marx, relations of production dominate every aspect of social life.

The criticisms of technological determinism arise out of the presumed role of forces of production over relations of productions. Forces of production, including innovations in technology, are said to have a dominant position over relations of production. Langdon Winner follows this line of argumentation and asserts that, ¨in most cases, Marx seems to be saying that there is a one-way influence between forces and relations of production¨ (Winner, 1978, p. 80). This line argument assumes that technological innovations are fixed in character. For they are fixed, technological artifacts gain their function prior to their implementation. From this follows the idea that technology is only capable of serving the interest of the bourgeoisie who owns and activates the process in which technology is developed.

Others refute that Marx's thinking is technologically deterministic. In *Capital* Marx writes that technology, ¨discloses man's mode of dealing with Nature, and the process of production by which he sustains his life, and thereby also lays bare the mode of formation of his social relations, and of the mental conceptions that flow from them.¨ (Marx, 1990) Marx explains the intricate relationship between technology and humans' relation with nature, reproduction of their lives and their relations and even formation of mental conceptions. However, that which lacks from Marx's account is a causal relation. Instead, Marx is interested in; as David Harvey puts it, how these aspects ¨interact with one another in the construction and reproduction of social order¨ (Harvey, 2003).

2.1.2 Technology and autonomy

Understanding technology as one of the elements in which material life is reproduced requires a conception of technology that accounts its adoption. Technologies are not always forced on human beings, and even in the cases where they were; there is still a great deal of resistance. Just because a new technology emerges, it does not mean that it will be accepted as given. Unfortunately, many technological determinists and their critics alike share this position. This position, in the words of Nick Dyer-Witheford, is defined as ¨technology-as-domination.¨ This position assumes the complete submission of subjects to new advances in technology, therefore taking the adoption of technology within the terms of domination.

Dyer-Witheford is exemplary of the line of thinking that seeks the place of agency in history of technology. According to him, technological innovations may attempt to solidify given existing interests; however, ¨capital's laboring subjects may find real use values, even subversive ones, for the new technologies¨ (Dyer-Witheford, 1999, p. 54). It is therefore crucial to account for the adoption of technologies. Uses of technological devices do not always follow their intended design functions. People are creative in finding new uses for technological artifacts, and it may be the case that innovators of technology do not presuppose new functions, or even that new functions are contrary to the design intent. Additionally, technologies can create modes of adoption that has not been predicted. These modes of adoption can transcend design functions, and therefore cause innovators of the technology new problems.

If we were to see the Internet as a technology that fundamentally dominates human beings, with reference to its original design intent of improving military communications, we would be turning our back to new forms of communication, organization and experience that the developers in the 70's would not be able to imagine. The Internet has evolved from a decentralized tool for communication for the well being of a centralized hierarchy, the army; into a space of socialization, a medium in which new meanings are invented rapidly. The Internet has become the venue of production, consumption, and circulation; of images, meanings, information and organization. It is no longer adopted into existing social processes; it creates the conditions in which it is further adapted to social order. And from the standpoint of the power, it requires strategies to regulate this process of adoption. The autonomy of Internet, and its adaption by humans, appears as an arena in which power governs.

2.1.3 Internet and governance

Question governance emerges very early on in the history of the Internet. Early scholars who wrote on the perceived nature and capabilities of internet communication quickly understood the underlying tension between individual internet users and governments whose funding has made the Internet possible (Barlow, 1996). In order to present counter arguments to state officials, early scholars relied on the idea that Internet has autonomy from political will of those in power. They did not frame Internet within a deterministic manner, and praised Internet's capacity to resist attempts to seize and control. Their ideas have contributed to practices and institutional formation that ensured a decentralized governing of the Internet. Formation of decentralized network of institutions and practices of governing has shaped internet technology, as we know it. Discussions global internet governance is crucial for setting the global conjuncture of this thesis.

One of the initial responses to the development of the Internet was based on a conception of Internet that was not subject to government. In this view, Internet was inherently ungovernable, due to its fundamental architecture (Musiani, 2013).

Some even took the idea further and offered that Internet can in fact disrupt governing bodies around the world, by rendering geography, distance and language irrelevant (Friedman, 2005). In this line of thought, effects of the Internet are reduced to its application in global trade. Initially seen as a tool that enables promotion of free market ideals and relations, Internet is argued to break boundaries imposed by nation-states. Thomas Friedman argues that not only Internet results in self-government of individuals, but also government on the basis of market ideals is better for public good. Such an argument prioritizes free market ideals over political ideals, and thus result in obscuring the political process in which internet technologies are themselves governed.

Friedman's fascination with globalization drags him along to fast conclusions that are detached from material conditions of, and possibilities posed by, his subject matter. David Harvey identifies such a fascination as a kind of fetishism (Harvey, 2003). All who study the relation of governance and the Internet does not share a fetishistic stance. They argue that Internet does not possess a capacity to act as a tool to be used to govern the political process of the nation states (Goldsmith & Wu, 2006).

The literature on the capacity of the Internet to contribute to governing of states, deals with questions regarding providing services to citizens on the Internet. Collectively called e-governance, the field does not contribute to the discussion regarding the government of the Internet. E-governance theorists take Internet simply as a tool that is to be used in increasing states effectiveness in governing.

Another way of thinking governance and Internet together has been put forward by John Perry Barlow. Barlow, in his 1996 essay, *A Declaration of the Independence of Cyberspace,* called out to "governments of the industrial world.¨ Barlow argued that Internet made possible organization of like-minded people. This new form of organization, as he calls is ¨civilization of the mind¨ is capable of governing itself, without any intervention of states around the world (Barlow, 1996). In fact, Internet would be a more humane place, if left to the self-government of the digital subjects.

Barlow's essay has been widely influential. It has provided many of the digital libertarians with tools necessary in arguing for the "un-governance" of the Internet. It is important to note that, while Barlow addresses directly to states, his formulation of the cyberspace is devoid of ¨legal conceptions of property, expression and identity¨ (Barlow, 1996). So the place of commercial interest in this ungoverned Internet is open to question. The model of governance dubbed as multistakeholderism was in development at the time of Barlow's writing. His text was written before the increasing power of commercial enterprises over issues of internet governance. Intellectual property has not become a dominant issue, in which companies used to exert their influence on the government of the Internet worldwide.

Barlow's conception of the future of the Internet resonated one of the fundamental ideas of those who saw in technology capacity for autonomy. Although, Barlow sees the Internet as a space and a medium rather than as a technology, the idea that freedom from intervention from the states around the world reflected a belief in affects of internet technology.

Where Barlow saw a utopian "civilization of the mind¨, his contemporaries, who had a keen eye on the economic developments giving the spread of the Internet a momentum, saw the interests of the transnational corporations. Herbert Schiller wrote, as early as, 1995, that "control of information instrumentation, invariably goes hand in hand with control of message flow and its content, surveillance capacity, and all forms of information intelligence. To be sure, the revenues from such control are hardly afterthoughts in the minds of the builders and owners of the information superhighway¨ (Schiller, 1995). Schiller, a contributor to information economy literature, shares the technology-as-domination perspective, meanwhile providing the general outline of the structure of interest in internet governance. In his account, U.S. state policy is to use

Internet to elevate national influence and interest, in the domestic and international arena. Corporate involvement in matters around Internet is a state policy, which grants state control, surveillance and intelligence capacity.

The political line U.S. followed on the internet policy was encouraged by the perceived contribution of the Internet to the sovereignty of the state. Contribution to sovereignty would be through increased economic power, which means use of the Internet to expand national and international markets. Schiller explains that, although sovereignty was the argument on the political level, in reality, transnational capital would be the major actor to benefit from the spread of the Internet, and hence, the increasing involvement of corporations in the matters of internet governance. In Schiller's account, corporate interest shaping the future of the Internet appears to be a U.S. state policy. This political strategy results in putting satisfactory governance in a crisis (Schiller, 1995).

As the intricate relations between U.S. government and the private sector lay out, technical experts of the field started their own debate on the internet governance. Especially after the Edward Snowden's revelations of mass surveillance conducted by NSA, the role of the state in internet governance emerged as a problematic issue. Even though the official line of the Unites States government was to keep away from decision-making responsibilities about the core issues, by way of transferring them to not-for-profit institutions such as ICAANN, it became clear this line of governmental strategies did not prevent government security agencies to monitor the Internet.

Although Snowden revelations have sparked a new initiative for reorganizing within the internet governance community; in the early days of initiation the Internet, state control was not a dominant theme in discussions. The main topic of discussion was that of the legitimacy. After United States policy of granting civil society institutions acting on the central issues of the Internet, the problem of representation in the governance instructions appeared. Until Snowden's revelations, these problems remain unsolved. For that reason, legitimacy was the first major issue academics studying internet governance addressed.

It appears that internet governance academics who were active in the institutional politics, formulated problems governance in terms of inclusion to decision-making process (Mueller, 2002). Hence, they were more inclined to think around the questions of ¨who¨ rather than ¨how.¨

Hence the question of legitimacy emerges as an important focus point in studies dealing with the governance question in Internet. The problem of legitimacy facing internet governance institutions has long been dominated by the question finding a ground to base the legitimacy of decision making. Internet is not a private property, nor is it under a direct legislation of one country. The United States Department of Commerce is involved in internet governance institutions, in the form of attending in some documents by means of signature, however, the Department does not interfere with the decision making process. The partial solution found for the legitimacy crisis was the model that was later dubbed as the Multistakeholderism[22]. The model was initially a design to involve varying actors around the world (Mueller & Wagner, 2014).

[22] Multistakeholderism is a model of governance, in which stakeholders participate in the governance process of a company or an institution. In internet governance, multistakeholder model corresponds to the inclusion of multinational IT companies, civil society organizations, professional associations, local citizen groups and nation state governments in the decision making process. In this model not-for-profit organizations act as legitimate governing bodies, in which representation of stakeholders take place. This model represents an alliance between civil society and private sector (Mueller & Wagner, 2014).

Nation states were present in this model, as well as NGO's, technical experts and technology companies. Even though participation of different stakeholders was the key, private sector appeared to have a higher hand. By being equals with state governments, private sector achieved a *de facto* greater power of representation.

Milton Mueller, writing from the framework of institutional economics, sums up the early conceptions of 'governance' within the policy-making circles. At once, it was used to mean "legal and organizational arrangements" (Mueller, 2002). Over time, with the increasing understanding of the root servers, that it could be used as a single point for the surveillance of users, a broader conception of governance emerged. This conception took an account of the fact that even though the object of government was a technological thing, a server, it could have an impact on the lives and resources of the individuals. Government of the DNS root server could mean that regulatory principles can be introduced specifically designed to exclude individual or collective subjects.

Mueller defines two axis of internet governance, with particular reference to the contradictions arising out of conditions peculiar to the Internet. Internet governance involves technical management and regulatory control (Mueller, 2002). Technical management is the kind of management necessary for the uninterrupted working of the root server. However, technical decisions, aimed at the wellbeing of the root server can have economic implications. Consider, for example, the market value of the name places, and possible funds a brand would pay to acquire its name domain on the Internet. It is then an aspect of the technical management that private stakeholders can try to assert their influence. On the other hand, the regulatory control is within the possible scope of the government of the root server. Owing to its central position, a root server can be used to collect information of users worldwide. With a little boost in the responsibilities as a regulatory force, governance institutions can end up controlling the Internet instead of governing it.

2.2 Limits of power and governmentality

Cyber security measures have gained a visible prominence in almost all topics that information technology experts work with. Topics ranging from efficiency of transaction of information to educational potentials of the Internet have been inserted into a security-oriented reasoning, which only relates to the topic at hand in terms of security.

Why approach the question of cyber security with concepts originating in theories of government? It is a matter of locating the agency in the development of field of cyber security. Concept of government enables for the identifications of actors involved in the field, without presenting them within a hierarchy in which one actor dominates all. Using the framework of government/governance was a necessity in the case at hand, particularly because of the persistent interventions of Turkish state into information technologies field for promoting security anxieties. Security anxieties came to dominate the field of information technologies the last few years. The scope of security anxieties implies that, measures taken towards ensuring cyber security do not take place in isolation from other kinds of developments. Security concerns became apparent in various spheres, such as in individual internet experience of citizens, in digital investments of commercial entities, in structuring of state institutions and in forming of civil society organizations focusing on information security. The wideness of the spheres in which focus has shifted to security implies that the way Internet is governed undergoes a change.

An aspect of the change at hand is that it does not simply refer to a change of conduct of institutions, individuals or experts. Increase of security concerns in internet governance brings about new institutions, along with it new experts positions and new individual conduct. It brings along constitution of a field of cyber security, which includes institutions, associations, experts and a discourse of risk. Fieldwork shows that strengthening of security concerns in the internet governance relies on creation of field of cyber security. In a sense, security governance requires new forms of institutions and expertise, so that internet governance can be directed into objectives of security. Cyber security field acts as a force that pushes security related agenda in internet governance circles.

What makes the concept of internet government distinct from the concept of internet control is that in the case of subjects, government provides more of a freedom, as opposed to the subjugated subjects under control. Government achieves its objective by working through those who are governed. By way of using the concept of government, I imply that the field that which is governed has a certain degree of freedom.

The concept of government, taken only to include institutionalized actors, state institutions, non-governmental organizations and actor of private sector has limits. Even though it offers a horizontal relation between these actors, and that this relation is better suited to explain field of cyber security than the concept of control, the process of government includes more than these established actors. Discourse of danger and risk is a crucial element of cyber security field; as well as militaristic narratives of cyber security breaches. Material conditions of internet infrastructure contribute to the governing processes, through the kinds of actions it allows actors to do. Software and hardware contribute to governing process, by making companies that sell them as actors of governance.

Adding this extra layer of discourse and technical elements, allows for a formulation of the governing process that exceeds actors and their interests. Internet governance process cannot be reduced to a simple play of opposing interests of actors. It should include level of capabilities that may allow or prevent the crystallization of these interests. Cyber security gains its importance as a strategy of power through capabilities it opens up. Therefore a broader concept of government that can include a wide range of social relations and technical capabilities is needed. The philosophy of Michel Foucault provides the necessary alternative perspective, particularly his concept of governmentality.

2.2.1 Foucault and the question of governance

Starting with a study of insanity in the mental hospital, medical practice and foundation of the prison, Foucault has studied forms of power; be it in the form of organizing knowledge, disciplining bodies or governing populations. Foucault's main interest in studying forms of power is to explain how we have become the subjects we are. For Foucault, the self is a side effect of power relations. We identify ourselves as subjects within operations of power. Thus we are always a part of flows of power (Foucault, 1990). However, this does not mean that we are captives, repressed under operations of power, waiting to achieve ultimate freedom. We can move towards freedom, but that requires operations of power, only for different ends. For Foucault, there is no outside of power.

In this approach, the definition of power is irrelevant (subsequently Foucault does not define power)[23]. Instead the significant thing is the ways in which power operates. In order to grasp how the world is the way it is, we need not know what power is. We only need to observe how it interacts with its subjects.[24] In order to pay attention to the ways in which power operates on subjects, we need to map out what Foucault calls "technologies of power". Technologies of power aim to shape the conduct of individuals, so as to create desired effects (Rose, 1999).

The crucial aspect of Foucault's conception of power is that it is not limited to prohibition. Power allows. It disciplines bodily forces and energies; and creates new ones if necessary or desirable. It can be a productive force; such that in its operations in the domain of knowledge, power encourages forms of knowledge that is essential to disciplinary strategies. Power establishes norms, which directs subjects in productive

[23] Although Foucault does not define the concept of power, he identifies certain forms in which power takes. Some forms of power become dominant in certain historical periods, which causes a mistaken account of these forms that categorize them as historical periods. Forms of power are not simply periodization. Because the elements that constitute forms of power are present throughout human history, operating with varying degrees of predominance within particular fields. The Turkish case provides plentiful evidence for the coexistence of multiple forms of power, even though they are contradictory to one another.
One of the forms is sovereign power, which is primarily concerned with prohibition through brute force on the body, a right to kill. Additionally, Foucault introduces two forms of "power over life" that are in effect from 16th century onwards in western societies. These are: disciplinary power, which aims at governing of the conduct of the individual body; and biopower, that aims at governing of the population (Foucault, 1990, p. 139).

[24] In his analysis of power and subjects, Foucault prioritizes the body. Power is distinguishable through its effects on the human body. Power kills or nourishes the body; disciplines, optimizes its capabilities, increases its usefulness; sees it as species body, as holder of life, and as population. For Foucault, power is not something that lingers up above, apart from us humans, who seek to possess it. It does not linger and it does not exist apart from humans. It is only visible at the point of its interaction with the human body.

actions that subsequently result in making of the material world. Power does not simply destroy; it also creates (Foucault, 1990).

When thinking of a productive power, we tend to think power in terms of particular institutions. However, power is not fixed in society. No institution or practice is the original embodiment of power. Hence power is not essential; it is not essentially situated at concentrated places. It is in a constant flow. "Power is defined as 'actions on others' actions:' that is, it presupposes rather than annuls their capacity as agents; it acts upon, and through, an open set of practical and ethical possibilities. Hence, although power is an omnipresent dimension in human relations, power in a society is never a fixed and closed regime, but rather an endless and open strategic game" (Gordon, 1991).

2.2.2 Governmentality

In order to understand how a thing can be governed, we have to explain Foucault's concept of governmentality. Because of the technical character of the field in question, we will have to make use of applications of governmentality approach to technological fields, particularly telecommunications technology. Secondly, due to the findings that indicate the state is directly intervening in internet governance, we need to lay forward the relations between the state and the concept of governmentality. Some of the objectives of security focused internet governance requires tools that enables centralization of power. Centralized character of, some state internet governance institutions and technical devices used in governing, enables us to think of security focused governing of technologies and authoritarian control together.

Foucault defines governmentality as the “art of government” or “governmental rationality.” It is an “ensemble formed by the institutions, procedures, analyses and reflections, the calculations and tactics that allow the exercise of this very specific albeit complex form of power” (Foucault, 1991, p. 103). Calculations, tactics, strategies are central to governmentality. This is exemplary of the indirect manner in which governmentality relates to subjects. Through indirect actions, governmentality renders subjects active in their self-government.

We should not be mistaken to treat the government as an entity; the relation to government and subject can not be reduced to the state and its citizens. Governmentality does not necessarily include state apparatuses, and when it does, it does not govern territory: it governs things. Foucault elaborates this point as such: “With government it is a question not of imposing law on men, but of disposing things: that is to say, of employing tactics rather than laws, and even of using laws themselves as tactics- to arrange things in such a way that, through certain number of means, such and such ends may be achieved” (Foucault, 1991, p. 95).

Even though government cannot be reduced to the state, it is possible to talk about the governmentalization of state. Speaking in 1987, Foucault explains the importance of governmental dynamics in contemporary politics in these words: “Problems of governmentality and the techniques of government have become the only political issue, the only real space for political struggle and contestation, this is because the governmentalization of the state is at the same time what has permitted the state to survive” (Foucault, 1991, p. 103). Governmentalization of the state makes governing practices and concerns inherent to government process the crucial reference point of politics. One can argue the political process is fixated on the governmental problems instead of ethical ones. For this reason, understanding the role of the state in governing is crucial. It is possible to think of the state as an element among others in the governing process, rendering it as an actor among others, in the constitution of our political present. However, I suggest that on a smaller scale, a field such as cyber security can emerge so as to allow the state as the central actor of governmental reasoning. In cyber security field, the state is de facto center for use and development of governmental strategies. Additionally, in a broader field, the field of internet governance in Turkey, the state is dominant enough to use cyber security as a technology of government. It is possible to talk of cyber security practices as a form of technology, one that which produces results in the image of governmental desires.

Michel Foucault's concept of governmentality has been taken up by a variety of academics. Among them, scholars from Anglo-Neo Foucauldian School[25] have a distinct position, for they undertake a project of extending the concept of governmentality in various fields, most importantly to political rationalities. In explaining our political present, Anglo-Foucauldians apply governmentality perspective to political practices.

Among Anglo-Foucauldians, Andrew Barry focuses on the role of technology in the practices of government. Barry identifies the increasing role of technologies in our political present. According to him, ¨we live in a technological society to the extent that specific technologies dominate our sense of the kinds of problems that government and politics must address, and solutions that we must adopt¨ (Barry, 2001, p. 2). Barry's

[25] Anglo-Foucauldian School is collaboration among scholars who critique instrumentalist theories of the state, through use of Michel Foucault's work on governmentality. Scholars critique a state centered process of government, and instead put forward a de-centered account of government, which accounts for the relative autonomy of institutional orders, from economic reductionism. Some of its leading figures are, Graham Burchell, Colin Gordon, Nikolas Rose and Peter Miller.

approach is useful for elaborating the intricate relationship between politics and technology; be it in the form of obsession with technological fix or technology induced political collapse.

According to Barry, technological problems appear to be political problems; as rulers increasingly concern themselves with maintenance of technological devices and practices. In this process it is possible to observe that, "specific technologies dominate our sense of the kinds of problems government and politics must address, and the solutions that we must adopt" (Barry, 2001, p. 2). Among the technological problems politics address are: maintenance of technological competitiveness, protection of intellectual property, dangers posed by unintended consequences of technological development, risks concerning e-commerce and e-democracy, public understanding of science and the necessity of individuals to indulge in life long learning in the face of technological change.

Maintenance of technological systems, including protection digital systems, is a crucial figure of contemporary politics for it is in close relationship with space of government: "centrality of technology to the reconfiguration of what one can call the space of government" (Barry, 2001, p. 2). It is possible to view the increasing anxiety over digital system security as a side effect of operation of government, "in relation to zones formed through the circulation of technical practices and devices" (Barry, 2001, p. 3).

Barry's work focuses on a particular strategy of government, one that which he calls "interactivity." Interactivity operates at the level of individuals, through encouraging them to immediately and physically participate actively in scientific experimentation, made possible by interactive technologies. Interactivity serves as a model for governing of and governing through technology. Relations between persons and information technologies follow an interactive path, according to Barry, which results in, among others, preventing engaging in critical reflection. Interactivity reduces the space for creative forms of passivity, and by doing so it promotes physical and practical connection, instead of messy and complex scientific practice (Barry, 2001).

Aside from being a form of technology, interactivity is the way in which objects and subject are organized in contemporary societies. It is "dominant model of how objects can be used to produce subjects" (Barry, 2001, p. 129). Production of subjects through interactive technologies relies on the active subject, who, in his own flexible time, engages with objects in brief interactions, by guidance (as opposed to rules) with the aim of maximizing possibilities for interaction. Injunctions directed to subjects are "discover" and "you may" (Barry, 2001, p. 150).

Information technologies make innovative ways of governing strategies available. Information technologies "enhance the self-governing capacities of society itself" (Barry, 1996, p. 128). Subjects are expected to be informed of issues regarding their bodies, technological devices they use, services they acquire and actions they partake.

Information technologies separate "rule" and "territory" from each other, rendering information flows as a space of rule (Barry, 1996). In technological societies, spaces of government are located within technological zones, which extend beyond borders of nation states. Technological zones are in process, for they require adjustment, regeneration and reconfiguration (Barry, 2001, p. 40).

2.2.3 Governing for security

With the flow of information emerging as a separate space of rule, strategies of power that are affiliated with territory should be revised so that they can still apply to technological field in which information flows take place. Among objectives of rule, security is one that can be detached from territory, and be made relevant to the domain of population. Population is the domain within which Foucault identifies strategies of power that reflect security rationality (Foucault, 2007). I think, space of rule opened up by digital telecommunications technologies can host security rationality and its related apparatuses, particularly those apparatuses that relate to the government of event.

Just as there are specific details that differentiates governing of technological societies from other domains of government, governing in order to grant security has tensions and techniques of its own. Michel Foucault himself has studied apparatuses of security through the examples of scarcity and epidemic. According to Foucault, apparatuses of security are distinguished by the way in which they deal with the "event," the world of phenomena.

Foucault explains three mechanisms which apparatuses of security make use of. Apparatuses of security "insert phenomenon in question within a series of probable events." The way in which power reacts to the phenomena at hand is then placed within a calculation of cost. And finally, apparatuses of security establish "an average considered as optimal on the one hand, and, on the other, a bandwidth of the acceptable that must not be exceeded" (Foucault, 2007, p. 6).

Apparatuses of security rest on an analysis that does not isolate targeted phenomena. Analysis of the object of problem is taken within the greater reality it is a part of, not simply at the moment it poses a security risk. Foucault explains this point through an example of scarcity of grain as a security problem. "The event in which one tries to get a hold will be the reality of grain, much more than the obsessive fear of scarcity (Foucault, 2007, p. 36).

Risk serves various social functions that are not limited to security rationality exemplified by scarcity. In fact, risk has entered in various domains within social relations, such that distribution of risk becomes the major problem of politics and management (Beck, 1992). In Ulrich Beck's definition of a risk society, calculation, production and distribution of risk emerge to be the central preoccupation in modern societies. Defining quality of modern societies has become its reflexive character; not a society occupied with its own development against an external force, but rather a society seeking development against the outcomes of its own being. Logic of risk production has come to dominate the logic of wealth production, resulting in the increasing difficulty of isolating risk in closed spaces and national borders (Beck, 1992).

Govenmentality literature has taken up the study of the concept of risk. According to literature, risk is distinct from dangerousness. While dangerousness implies an internal quality of the subject, whose well-being is the main objective, risk relies not on the subject but on the factors that can act upon the given subject. Therefore, risk is the " effect of a combination of abstract factors which render more or less probable the occurrence of undesirable modes of behavior" (Castel, 1991, p. 287). Risk brings about strategies of power that focus not on individuals but calculations, factors and correlations. Calculations of risk require information flow from surveillance technologies, so that data can be used to "multiplication of possibilities for intervention" (Castel, 1991, p. 288). Through calculations of risk, operations of power can intervene in personal and collective conduct in the name of eliminating risks. Risk can be used in producing docile subjects. In this sense it can serve as a disciplinary force.

Concept of actuarialism is developed to emphasize the preventive uses of risk in disciplining subjects. While others argue for prudential forms of power, which invites subjects to be rational and responsible and in partnership with experts active in the process of distribution of risk (O'Malley, 1996). Strategies of prudential power correspond to a change in understanding of risk, which is in contrast to disciplinary forms of power that is primarily geared towards elimination of risk. No-risk society that is governed by a welfare state model relies on distinct strategies of power from those governed by security. Risk calculation, can be a part of strategies of security, but not unconditionally, for logic of risk calculation can create unseen opportunity and change rather than eliminating risk (O'Malley, 1996).

Apparatuses of security rely on techniques that do not seek to prevent an event from happening, but rather to "arrange things so that, by connecting up with the very reality of these fluctuations, and by establishing a series of connections with other elements of reality, the phenomenon is gradually compensated for, checked, finally limited, and, in the final degree, canceled out, without it being prevented or losing any of its reality" (Foucault, 2007, p. 37).

So in the way Foucault describes it, techniques of security are not concerned with preventing dangerous event, but rather to eliminate and cancel out its effects. There may still be danger-posing phenomena, but they are viewed not singularly, but rather as a part of a whole, in which its effects can be nullified. This is, in a sense, a liberal strategy, as in letting things to happen. However, letting things happen does not bring nullification of the phenomena on its own. So apparatuses of security ¨tries to work within reality, by getting the components of reality to work in relation to each other, thanks to and through a series of analyses and specific arrangements¨ (Foucault, 2007, p. 47).

The problem of security often comes about as a result of the ways in which things and people circulate. It is circulation of goods in the case of scarcity, and circulation of contagion in case of epidemic that makes these a problem of security. Circulation, Foucault explains, in the broadest sense ¨of movement, exchange and contact, as a form of dispersion and also as a form of distribution.¨ Security apparatuses “ensures circulation of things, in such a way that inherent dangers of this circulation are canceled out¨ (Foucault, 2007, p. 64-65).

2.3 Academic literature from Turkey on the Internet

Since the early days of introduction of Internet in Turkey, academics have written consistently about the new technology. Early academic studies about the Internet include quantitative studies on spread of internet connectivity and analysis of application of internet in education, commerce and bureaucracy. As years pass by, themes that direct academic writings multiply, so as to include effects of Internet on society in various spheres.

Early examples of academic studies by social scientists about Internet in Turkey provide a statistical account. Quantitative studies provide evaluation of internet connectivity, computer ownership, and society wise internet literacy (Aydin, 2001; Ozgit & Cagiltay, 1996). Growth of internet use appears to be a central issue of these studies, since economic model of internet service provider companies are studied in reference to spread of internet literacy. Forming of an efficient telecommunications market in Turkey is seen essential for spread of the internet service (Wolcott & Çağıltay, 2001).

There are studies reflecting an educational perspective. Statistical researches have included use of Internet for educational purposes in schools and universities (Aydin, 2001). A comparative approach has been used, in comparing Internet use in schools to rest of the world (Usun, 2003). Educational potential of Internet has been recognized, and has been a policy matter for academics working in children's education (Tuncer & Yalcin, 1999).

As the internet connectivity spreads through various segments of the society, researchers begin to study effects of internet use in professions and individuals. Profiling of internet users is significant part in these studies, such as internet café users (Gürol & Sevindik, 2006; Eskicumali, 2010). These profiles reveal the ways in which Internet is used among youth. Youth internet use is seen by some researchers as problematic. As the Internet can be a tool of education and personal development, it can as well be a substance of addiction (Ozmutlu, Ozmutlu & Spink, 2008). Other researchers focus on Internet use for medicinal purposes, such as consultancy in pregnancy (Kavlak, Atan, Güleç, Öztürk & Atay, 2012).

There is a major division within the sociology of Internet, between sociologist who frame the Internet as a form of technology and those who frame it as public space. Framing of the Internet primarily as a space in which persons interact with each other has been taken up by academics from Turkey. Focusing on problem of political participation, research has been made that view Internet as a space, cyberspace, in which activism takes place. Youth activism on the Internet is related to activism in real life (Karabag & Coskun, 2013). Cyberspace can also be a space in which identity formation occurs. With providing relative freedom and visibility to suppressed identities, cyberspace contributes to formation of gay and lesbian identities and activism (Gorkemli, 2012). Conversely, cyberspace can act to destabilize borders between national identities. It can provide a space in which those who want to discuss and deconstruct national identities (Theodorelis-Rigas, 2013).

In addition to topics outlined above, questions of internet security attract academics working on the effects of internet in Turkey. Internet security is handled through various frameworks, such as children's use of Internet and potential risks they may encounter (Karakus, Çagiltay, Kasikci, Kursun & Ogan, 2014). The way safety is conceptualized in these studies is similar to the ways in which ¨safe-internet¨ is discussed in contemporary politics. In this vein, parents are seen inadequate to protect their children from risks.

Alongside of the studies focusing on internet users safety online, there are studies focusing on system security management in Turkey. Researchers have analyzed the current state of information systems security of the public institutions, and have found that the lack of legislative measures regulating systems security hinders the development of practices of system security (Ozkan and Karabacak, 2010).

While researchers of management of system security calls for more legislation, in the case of internet censorship, calls are not for more but to-the-point legislation. Prior to passing of law number 5651, lack of jurisprudence appears to be a major problem, which results in cases that frame Internet inherently as a tool for crime (Altintas, Aydin & Akman, 2002). After the passing of law number 5651, researchers of internet law have provided critical assessment of the law, and the ways in which it enables censorship (Akdeniz & Altıparmak, 2008).

2.3.1 Turkey and politics of internet governance literature

Some of the internet governance literature from Turkey focuses on information society developments. EU membership process accounts for a great deal of information society developments, which follows neoliberal governing rationalities. However, Turkish case is not limited to neoliberal government. Turkish case illustrates ways in which authoritarianism and neoliberal governing rationalities coexist (Topak, 2013). Intricate relations between authoritarian and neoliberal governing rationalities results in citizens connected to global information flows while kept under digital surveillance.

Özgün Topak studies current governing of Internet in Turkey through the workings of experts, Justice and Development Party and European Union. Through the interplay of these actors, a restructuring of economy and state occurs. The plurality of actors is crucial in the introduction of neoliberal governing rationality. Each actor has a distinct position that makes the combination of neoliberalism and authoritarianism possible. The proposed shrinking of the state in the neoliberal theory is coupled with surveillance strategies. Surveillance, while not of central importance to scholars of neoliberal governmental rationality (Rose, 1996), becomes a crucial technology of government in the Turkish case.

Topak argues that regardless of their political preoccupations, actors active in the governing of the Internet in Turkey, seek to create active subjects, whom comply with neoliberal values of competition, flexibility and mobility (Topak, 2013). In Topak's account, coexisting authoritarian and neoliberal governing strategies make use of a conception of technology that is essentially empowering to the individual. These technologies make possible the decentralization of the state, in compliance with neoliberal governmentality.

Aside from information society approach, the politics of the field of Internet has drawn particular attention. Internet is an important field for the organizations and self-representation of dissident politics. Politics of internet field, or rather of digital technoscape, and its relation to dissident movements is necessary to understand the current condition of the Internet. Turkish state relies heavily on surveillance practices in shaping of the Internet, particularly in relation to dissident politics (Çelik, 2015).

Burçe Çelik explains that while surveillance emerges to be the dominant method for controlling dissident politics on the Internet, practices of surveillance face resistance and negotiation. This allows for dissident subjects, particularly from Kurdish political movement, to manage their position in relation to forms of power (Çelik, 2015).

2.4 Theoretical inferences from literature review

The review and exploration of sources in this chapter allows for bringing concepts from diverse fields of theoretical research in for use of this thesis. Some of the concepts ensure that this thesis does not fall into theoretically unsound formulations of phenomena studied. Review of technological determinism has ensured that this research does not form a one directional relationship with cyber security field and general social and political processes active in Turkey.

Governmentality is the central concept that this thesis relies on. In order to identify cyber security as a strategy of power, this study had to provide an detailed account of the concept and the related theoretical work it is based on. As governmentality opens up a vast area of study, the relevancy of concept of governmentality to field of technology had to be documented through relevant sources.

The theoretical inference this study deduced from the literature review is that concept of government, and the larger formulation of governmentality can be applied to and narrowed down to study of technological fields that embody strategies of power related to security rationality. The rest of the thesis will try to provide empirical data to weave together these three concepts: governing, technology and security.

Concept of governmentality is relied on to define the general field of actors and influences, within which cyber security measures is located. Governmentality also provides an outline to locate the relations within field of internet governance, and establish meaningful links between state actors, private business actors, actors of civil society, discourses, developments of recent history, laws and technical artifacts.

The idea that technology forms a space of rule allows for applying theoretical elements of governmentality to field of internet governance and cyber security. While cited theoretical work uses concept of interactivity and focuses on human-technology relationship, this study focuses on relationship between technology and governing of technology. Reflexive relationship between the Internet and cyber security technologies allows defining cyber security as a strategy of power as a particular strategy of power that can bring security rationality into technological space of rule.

Concept of security rationality and security apparatuses are applied to the governing of internet technology, through application of the strategies of power affiliated with governing of the event to technical practices that cyber security performs. Event is based upon reflexive relation between cyber security practices to internet infrastructure. With security risks arising from internet infrastructure becomes the event of internet governance, cyber security appears as a strategy of power that performs functions put forward in Foucault's formulation of security apparatuses dealing with unwanted event.

Cyber security exceeds its function as a strategy against the event, and becomes an element in internet governance in general, for it provides technical capabilities that no other field presents to the field of governance.

CHAPTER 3

SECURING INTERNET

This chapter explains how cyber security measures form a technology of power. Through an analysis of legislation and state institutions, it seeks to lay out a foundation to frame the ways in which cyber security practices affect and shape reality. Cyber security measures can be framed as a technology of power, for they relate to governing of the Internet in general, insofar as they open up certain possibilities, and close off others.

In recent years, we see a change in the kind of problems that consider Internet as an element. In simple terms the change is that the Internet is referred to be the cause of many problems to society, to state, to security. This was not always the case. Internet was viewed as a domain of freedom and self-development, something that which state and civil society actors agreed on its benefit to society. This view has changed, I argue, and two critical moments have been definitive. The significance of these moments rest in the distinct ways they promote security rationality and practices. There has been a morality oriented turn towards security, which became dominant around 2006. Afterward a turn to security rationality that was based on technical necessities followed and became dominant 2011 onward.

As I shall demonstrate in this chapter, these two moments have been effective in shaping the way the Internet is perceived in Turkey. Not limited to the discursive level, the practical implications of these moments have changed the actors, the technological base, legislation, civil society stances and resistance on the Internet. Such that, actors have been realigned in their capacity to participate in the security practices. Legislation has been passed and legal ties have been found with the European Union. Technological infrastructure of internet service has been incorporated into surveillance technologies and militaristic defense expertise. NGOs have been formed to comply with security practices and educate and encourage a base of security experts. Resistance has taken a technological turn as well; leaking into state systems of publicizing classified information, often revealing the limited capacity of the state institutions in securing their own digital systems.

Cyber security concerns contribute to a dominant sense of what composes a political problem within the field of internet governance in Turkey. They are at once solutions to problems arising out of flow of undisclosed information. The shift towards security concerns and system protection in internet governance circles reflect the political issues that information leaks cause. Strengthening cyber security measures is a governing strategy that includes creating a force against forces that intends to unearth classified information.

Yet cyber security measures do not fully solve the problems they intend to solve. Therefore, we would be at fault to treat these actions as final products or tools that have achieved their goals. In the acts of protection of state owned digital systems, cyber security concerns exemplify governmental concerns that stand in the intersection of security. The distinctiveness of the cyber security case in Turkey is that it allows for a study of phenomena at the intersection of security, government and technology.

This chapter seeks to provide a general framework of security practices and rationality for further research. Among the greater phenomena that can be linked with securitization of the Internet, it concentrates on how legislative base of such turns came to be, and how state institutions have evolved to comply with security necessities.

3.1 Cyber security and cyber crime

Simply put, cyber security is about protection of digital information systems from forces external to the system in question. It includes several levels; software security, hardware security and signal security. Cyber security experts aim to prevent access to system functions by intruders, just as they aim to protect information held within digital systems. Information in question can be users' personal data or commercial data, which can be of value to outsiders. Security is activated in the face of a possible threat. Even when there are no threats, cyber security is still needed for threat may appear any moment, or so some cyber security policy makers argue.[26]

Various forms of information are stored in digital systems. Among stored information are primarily personal information, which can be anything from citizenship information kept by state agencies, to medical information held by hospitals and ministry of health. It can be the digital traces users leave behind as they surf online. Some of these are called metadata[27], which is simply information about information. Just as pieces of metadata can be arranged in a way to reveal the actual content, personal information held within systems can be used to locate individuals in question and affect their lives in the physical world. Security of individuals requires that their personal

[26] There is a great deal of anxiety about cyber security, and most of which, it is argued, rests on a somewhat exaggerated account of the threat in question. Accounts about presence of cyber threats, even when there are no actual attacks, are viewed to be ungrounded and to be a part of "military-industrial complex playing on" public fears (Brito & Watkins, 2011).

[27] Metadata is information that gives technical details about the way in which information in question has been produced or circulates. If we are to think of a telephone conversation as information, metadata would be everything except the contents of the conversation: the length of the conversation, the devices in which speakers used, the signal towers they have been connected to, etc.

information should be kept private, cyber security agents aim to prevent the leaking of such information.

Additionally, cyber security measures are employed to restrict network functions to those who are authorized. As machines and tools are often controlled through digital networks, cyber security measures aim to prevent outsider access to networks in question, so that machines connected to the digital systems cannot be controlled by others.

While the definition of cyber security can be as simple as protecting a digital system from forces that would disrupt its workings and the secrecy of its contents, particular ways in which cyber security is practiced is not as simple. From early days on, system security has always been a part of the trade of computer experts. As the technology evolved, its use in society has changed. As Internet became a crucial infrastructure for business transactions, the approach to security changed. As nation states relied more and more on internet technology, understanding of cyber security changed further. In this sense, cyber security is very closely linked to historical development of digital communications and its social organizations that make it possible.

It is possible to identify three strains, or rather three approaches to cyber security. These approaches put forward distinct accounts of who the main actors are, what the object that which to be secured is, and who or what poses a danger or threat. These three approaches are present today within cyber security policy circles. However, as this thesis argues with reference to fieldwork in Turkey, some of these approaches are gaining an upper hand. According to Myriam Dunn Cavelty, these three approaches are called: technical, crime/espionage and military/civil defence (Dunn Cavelty, 2012).

Technical discourse of cyber security has its roots in the earlier days of the Internet (Spafford, 1989). It has been materialized after a malware has affected the precursor of the Internet, ARPANET. Malware has rendered a proportion of the network unfunctional, revealing the fragility of the computer networks. Following this event, computer experts in charge in the early days of the Internet started taking security measures.

This early discourse of security predominantly focused on technical issues. It viewed malwares, viruses, Trojan horses and worms as the actual object of threat. As these were developed and used by people, the threat was argued to come from hackers. So computer experts and anti-virus industry appeared, and took hold in the technical discourse of cyber security. The object of security was simply computers and computer networks according to this discourse (Dunn Cavelty, 2012).

Technical discourse has its roots in a particular period in the history of the Internet. Before mass commercialization of Internet, and before it penetrated daily lives of the majority of the urban population, Internet was thought to be an arena of unrestricted self-expression and freedom. Techno libertarians developed this conception in the early days of the Internet. It stated that state interest and influence cannot and should not be present in the shaping the future of internet technology. As a space of unrestricted self-expression, Internet was not immune from security risks. The object of security risk was the individual computer and the network it was connected to. Need for security was to be attained from the market, through purchasing anti-virus software.

The second approach, crime/espionage discourse brings with it a different set of practices, a different set of actors and a different set of priorities. It relies on the needs of the commercial sector. In order to make Internet a reliable medium for conducting business, the discourse of crime/espionage has argued for the use of laws, and respectively, the intrusion of law enforcement agencies in digital communications. This was also argued to be necessary for the protection of state-owned networks. Just as commercial information should be guarded, crime/espionage discourse said, so should the classified data belonging to the state. Law enforcement agencies and intelligence agencies are to be seen as the main actors of cyber security in this discourse. According to this approach, threats come from cyber criminals. As legislation has passed, the category of cyber criminal framed those who use Internet as a means of fraud or theft (Mungo & Clough, 1993). Foreign intelligence agencies are also seen as a threat.[28]

The third approach, the military/civil defense approach, is based on the conception of internet communication as an element of warfare. This approach assumes an ongoing information war, and that it accompanies actual warfare. Digital systems are viewed as spaces of possible vulnerabilities that can affect society and strategic position of the military. The source of risk is the "enemy" in this approach, which can be state and non-state actors. Objects of risk are critical infrastructures; nuclear power plants, dams and crucial industry. Protection of critical infrastructure is necessary for maintaining the militaristic capacity of the host state, as well as the well-being of society (Rattray, 2001). The military should also be capable of protecting its own information

[28] It should be noted that dominant approach in Turkey is crime/espionage. Since 2006, passing of relevant laws and establishing of police divisions for the enforcement of these laws is exemplary of this fact. Research has shown that the methods of crime/espionage approach are still in the making, however.

systems. Principle of self-protection is often extended to include aggressive acts of cyber warfare.

In recent years, several countries established cyber war commands, for conducting cyber attacks on research projects and crucial information systems of opposing states (Dunn Cavelty, 2014; Dunn Cavelty, 2012). Responsible actors, according to the military approach, are the military and national security agents.

Aforementioned approaches lay out the broad range of the problems and solutions that cyber security experts identify. It is important to mention that Dunn Cavelty views cyber security from the standpoint of the state policy making apparatuses. While above categorizations are essential for making sense of and opposing the increased militarization of Internet, my field work reveals that in Turkey, demands of commercial sector is just as crucial as state actors in the making of cyber security field. Majority of the computer engineers specializing in cyber security find employment in the private sector. So while Dunn Cavelty's approach is helpful to understand governments' approach to cyber security, it does not explain the day-to-day trade of cyber security experts. This is an issue that I will return to when I discuss the Turkish case in detail in the following pages.

To ensure security, cyber security experts inspect digital systems in order to find weak spots. Cyber security work relies on a disciplined work of evaluating parts of the digitals systems, scanning code on which the system is built upon, and trying to estimate what an infiltrator can do. Inspection of third party software used within systems is crucial for cyber security. Third party software might have zero-day exploits[29], and cause vulnerability, even though the system running the software is fully secure.

A brand of cyber security experts called white hat hackers simulates a hacker's point of view when they are searching for vulnerabilities in digital systems. These experts are often placed against black hat hackers, from whom they differ by working for the protection of the system and not the other way around. White hat hackers sell their expertise to companies that seek to strengthen their digital systems. They evaluate and fix the system they are hired to check. Companies that conduct business online have security experts that are employed full time.

Day-to-day conduct of cyber security officials exemplifies a crucial point that Michel Foucault makes in his definition of security apparatuses. The daily work of cyber security is closely linked to the material aspect of the digital technology. They are working with what is already present, rather than an ideal in which they follow to make digital systems safe. A normative approach to internet technologies is hard to find in cyber security circles. Instead, a close inspection of digital systems at work, an estimation of the ways in which these systems can be hacked into is observed.

One of the primary reasons why we can frame cyber security practices as a technology of power rests in their shared characteristics with those, which Foucault attributes to security apparatuses. Michel Foucault defines nullification as the primary strategy for security apparatuses. In order to nullify a source of danger, government has to "grasp them at the level of their effective reality" (Foucault, 2007, p. 46). Security strategies move from not an ideal image or an end. Instead, they take the situation dealt

[29] Zero day exploits are a kind of vulnerability that can be found in software. These are not released to the public or are unknown to the author of the software. So once they are made public, there is no present solution to the problems they cause.

with as a starting point and responds to it by using other existing forces. If breaching of digital systems is the security problem, security strategy accept the problem as it is, and locate against it another domain, that of cyber security field, so that it cancels out the efforts of the hackers. Foucault explains the nullification process in these words: "the law prohibits and discipline prescribes, and the essential function of security, without prohibiting or prescribing, but possibly making use of some instruments of prescription and prohibition, is to respond to a reality in such a way that this response cancels out the reality to which it responds-nullifies it, or limits, checks or regulates it" (Foucault, 2007).

3.2 Cyber security in global internet governance policy debates

Debate on the role of governments in shaping politics of the Internet, persists among politicians, NGOs and academics who work on internet policy. Current Internet governance policy involves relative autonomy of the Internet from governments across the world. Although the technology of the Internet has been developed in the US, today, institutions that are crucial in functioning of the Internet remain independent of governments.

In the wake of Edward Snowden files, the current internet policy is in a crisis. The revelations of Snowden's documents, that the NSA has an extensive surveillance and spy network, that runs through almost the entire internet traffic around the world, has shattered the dreams of those who believe Internet is by nature an uncontrollable domain.

It is necessary to outline some crucial institutions that govern the technical infrastructure of the Internet. These institutions provide the technical labor and expertise necessary for the well being of the Internet. Institutions are at the center of the current debate on internet governance, in which Snowden leaks have changed the standing of the actors drastically.

The global internet governance debate centers around two opposing camps. These camps are constituted of actors of different levels. One camp is composed of state actors, and the other camp is composed of NGOs and the private sector. These camps have conflicting views on the role of the state and private capital in global government of the Internet.

State sovereignty camp is composed of state actors, mostly from developing countries. China, Brazil, Russia and South Africa are among the countries that support the national sovereignty approach in matters regarding internet governance. According to the internet policy researchers Milton Mueller and Ben Wagner, countries that share the state sovereignty approach "tend to be critical of US global hegemony and unenthusiastic, at best, about the so-called multistakeholder or private sector-led internet governance institutions, which they see as creatures of the US. They favor locating global communications and information governance functions in intergovernmental institutions such as the UN and the International Telecommunications Union (ITU). Some, but not all, of these states are authoritarian and fear Internet freedom" (Mueller & Wagner, 2014, p. 3). These states prefer locating international communications in intergovernmental institutions such as the UN and the ITU. In addition, these states voted in favor of ITU's revised International Telecommunication Regulations (ITRs) at the 2012 World Conference on International Telecommunications (WCIT) (Mueller & Wagner, 2014).

It appears as though there is relevance between cyber security concerns voiced in the international arena and state actors advocating for the increased power of nation states on internet policymaking process. State actors often refer to cyber security risks as a threat to national sovereignty. Developing countries that argue for the recognition of national sovereignty on the Internet frame the security threat in terms of cyber war. Discourses of cyber war render an image of Internet as a war field. According to cyber warfare logic, that which controls the global internet infrastructure has leverage against opponents in the cyber war. Countries such as Brazil, Russia, India and China look for a different kind of balance in internet governance, and cyber security is at least one of the causes that they reference to (Jamart, 2014, p. 66).

Cyber war is defined as a war of espionage and sabotage among nation states using digital telecommunications. Acts of cyber war include stealing critical information from state databases and sabotaging the workings of selected sites by bringing their technological infrastructure to a standstill.

Cyber war differs from cyber security in several ways. Unlike cyber security, cyber war relies on a militaristic discourse. Actors of cyber war are nation states, which makes cyber war an issue of international relations and diplomacy. Several states take cyber war very seriously, particularly, US, China, Russia, Iran and Israel. These countries employ, within military, a company of computer experts, whose primary job is to infiltrate into rival countries' digital systems, and to protect national systems[30] (Brito & Watkins, 2011).

The institutional body that is a part of the internet governance circles that are occupied with cyber security is International Telecommunications Union (ITU). ITU established the ITU Global Cybersecurity Agenda, after 2010 WSIS meetings resulted in Action Line C5, which is concerned with "building confidence and security in the use of information communication technologies." The organizational structure of the ITU reveals that the institution works through nation state based membership.

Even though cyber security is a policy topic that is used by states that support sovereignty, it does not have a clear outline. As mentioned above, there are institutional declarations and agendas, yet these are not coupled with a globally shared understanding of collaboration. Innovations that are made in the policymaking process are lacking within the security sphere. Currently, "official internet security polity is designed along the trodden paths of public-private partnerships and national security provisioning by traditional security institutions" (Schmidt, 2014). According to the scholars of the security policy field, what is missing is an institutional architecture.

The other camp promotes the "multistakeholder model" for internet governance. NGOs and private sector actors are allied in arguing for the multistakeholder model. Present internet governance institutions (ICANN, IETF, Regional Internet Registries and Internet Society) are in alliance with multinational communications and internet companies such as Verizon, Google, Facebook, and Microsoft. Also in this camp are state actors of European countries, Japan and the US. Governments in this camp voted

[30] Turkish state is among those states that prepare themselves to cyber war. According to information shared by Industry and Commerce ministry Turkish state employs 69 hackers as of 2013, which they aim to increase to 200 (Hoşgör, 2013).

against the ITU's International Telecommunication Regulations in 2012. NGOs in this camp are those who promote internet freedom and privacy. The NGOs from the sovereignty approach camp do not often share the views of their countries' governments.

Among institutions that are active in governing the Internet are ICANN, IETF, W3C and Internet Society. These are nonprofit organizations that are formed for the purpose of governing of the Internet in the early days of the technology. ICANN, Internet Corporation for Assigned Names and Numbers, is one of the most influential organizations in internet policy debates. It is cited to be the primary body that governs the Internet. The institution was born during the 90's when Internet was evolving into a mass medium. At the time, Internet Domain Name system, which is the technology to assign namespaces on the Internet to fixed IP addresses, did not have centralized governance. Nor was there a legitimate policy-making authority over the central issues of the Internet (Mueller, 2002). US government, instead of working through international treaties or public control, offered a model in which a private corporation controls the administration of the DNS. Attempt to achieve collective legitimacy for ICANN failed and legitimacy was supplanted by a privately brokered deal between the president of ICANN at the time, Jon Postel, Network Solutions (which operated the authoritative root zone server and the .com domain) and the U.S. Department of Commerce (Mueller & Wagner, 2014, p. 6). Despite disputes regarding the legitimacy of the institution, major decisions on the future of the Internet are handled by ICANN.

The second most influential institution in governing of the Internet is Internet Engineering Task Force (IETF). IETF is responsible for developing technical standards in which internet communication takes place. IETF also promotes standards regarding the technical aspect of internet communications. It is the institution that governs the technical infrastructure. IETF also assigns protocols, such as the crucial TCP/IP protocol or pop2 email protocol.

IETF consists of technical experts, organized in an open manner. Development of standards takes place within email lists, to which anyone can join. It is based on voluntary labor. Founded in 1993, IETF functions within the Internet Society.

Multistakeholder model is a discourse aimed at providing legitimacy for the ICANN. Ever since its establishment, the problem of representation within ICANN remains unsolved. Although it is a nonprofit corporation, there are still problems as to determining who will be active in the decision-making process. The solution was to include stakeholders from different countries in the policy-making organs (Mueller & Wagner, 2014). In the early days, this model was called "private-sector led governance." After the World Summit on the Information Society (WSIS), governance was redefined to include, technical experts, NGOs and businesses. On paper, multistakeholder model argues for governance of the Internet through non-state actors. The technical community, business and human rights organizations are thought to be active in the process of decision making. Although the intention appears to be libertarian, the problem of representation provides the conditions in which private sector actors exert their influence in the process of policy making. The institutional design of the ICANN, claiming to represent nation states, NGOs and companies, is not necessarily able to represent all view on internet governance. This became apparent when in 2014 Internet Governance Forum in İstanbul failed to represent all points of view on the internet policy.

The Snowden revelations provided state actors in the internet policy debates a chance to shift alignments within the field. In the wake of the revelations, internet governance institutions published a statement in Montevideo condemning NSA's activities. The Montevideo statement prompted institutions to distance themselves from the US government in relation to mass NSA surveillance. After Brazilian President Rousseff's strong criticism of the US for the revelations, Roussef and ICANN's president Fadi Chehadé joined in a call for a summit in Brazil. By way of a call, Brazilian President was making compromises from the sovereignty position and ICANN president Chehadé was signaling compromises to the multistakeholder model (Mueller & Wagner, 2014). This meeting is seen as a sign to provide sovereign states, which are critical of the current internet governance, "an equal footing" among business and NGO stakeholders (Mueller & Wagner, 2014). Interests of the multinational capital were disturbed. And within the ICANN as well, there appeared signals of new alliances, among those of in opposition (Mueller & Wagner, 2014).

New alliances among actors of multistakeholderism and state sovereignty did not bring a new method of policy-making method. The institutional design of the ICANN did not change in the aftermath of the Snowden revelations. The Brazil meeting between president Rousseff and ICANN president Chehadé resulted in a new summit, however, this summit did not appear to bring new forms of decision-making process innovations (Mueller & Wagner, 2014). Instead, IGF remained as the venue for internet governance policy making. Even though internet policy-making actors invent new venues for developing new ideas for governance. Developing nations and international NGOs are displeased with the role IGF hold in terms of policy making. Internet governance institutions have a great deal of power over the IGF process. Especially the program committee of the IGF is under control of these institutions. This condition affects the ways in which new debates are started over the core issues of the Internet. There are even blocking attempts of outcomes or recommendations (Mueller & Wagner, 2014).

Among the efforts to contest the condition of IGF, an effort by the British Foreign Office is relevant to the discussions on cyber security. The Office organized London Conference on Cyberspace in December 2011. Actualized as a series of annual cyber security-focused forums. These state actor-led conferences brought into the internet governance discourse the policy networks oriented around national security and foreign policy. They were designed to address "norms of behavior that govern interstate relations [...] in cyberspace" (Hague, 2011, as cited in Mueller & Wagner, 2014).

London Conference on Cyberspace is not the only case in which state actors have voiced out concerns about cyber security matters in relation to internet governance policy. International Telecommunications Union (ITU) lobbied for adding in International Telecommunications Regulations treaty concerns about cyber security. These additions sought to increase the authority of ITU on the Internet, especially about cyber security measures (Mueller & Wagner, 2014).

ITU organized World Summit on the Information Society (WSIS) from 2006 to 2013. WSIS provided developing countries and international NGOs working on issues revolving around the Internet, a medium to voice their criticisms of the governance model that has ICANN at the top. WSIS process, "gave certain developing countries and Europe an opportunity to openly challenge the legitimacy of the institutional innovation that was ICANN" (Mueller 2010, p. 60). Framing WSIS as an event in which state sovereignty actors tried to exert their influence would be incorrect. WSIS was organized in accordance with the ideals of multistakeholderism. However, the event mobilized both sovereignty actors and actors from the multistakeholder bloc.

While sovereign states use cyber security concerns to critique the multistakeholder model in internet governance, the issue they handle lacks a model. In fact, the current cyber security field lacks a policy making authority, leaving it as a free flow of security companies and target nations and companies (public-private partnerships), much like the multistakeholder model.

3.3 Two moments of security-focused internet governance in Turkey

While government strategies in Turkey arise from very local problems, as it is easily detected in the above review of the global discussions on internet security, they find correspondence in global politics of internet governance. Efforts towards securing the internet, and increasing the capability of the state institutions to control and intervene in the internet traffic, fit in the framework of those who argue for national sovereignty of the states on the Internet.

It is possible to talk of two significant moments in the governance of Internet in Turkey. These two moments of the recent past play a crucial role in the overall experience of internet users in Turkey, as well as a change in methods and strategies of internet governance. While a more comprehensive periodization would include more than just two significant points[31], I argue that these two moments, which I pin down to

[31] Arguably, the political changes these two moments reflect are limited to field of internet governance in Turkey. If we were to close the gap between broader political field and internet governance, we can pinpoint the year 2009, when large-scale trials have resulted in the imprisonment of thousands of Kurdish politicians and activists. It is possible to see these KCK trials as recourse to use of security strategies in

the years 2006 and 2011, are significant points reflective of the increasing gravity of security rationality in internet governance.

These two moments are the passing of law number 5651 in 2006 and the introduction of nationwide internet filter in 2011. Both of these events aim to control the information traffic on the Internet. While the first moment aims to control the sensitive content of information traffic, the latter moments shift the focus to actors of the information traffic and their infiltration capability. It appears that the shift somewhat signifies a change in the state policy. Even though this is the case, these two moments shape the whole field in which internet governance takes place. Therefore, it is still possible to make sense of these moments as changes in the governance field, rather than a policy of the one dominant actor in the governance. It is crucial to note that, even though I call these developments "moments" they to not signify singular events, but rather developments in time that share a common purpose.

It is possible to pin down the emergence of the first moment with beginning of child pornography debate in 2006. Child pornography became a high profile matter at the time with a high-level public support emerging to fight those who deal in child pornography. Public support was used to pass the first law that regulates the internet content. Law number 5651 brought along possibilities and responsibilities to censor websites.[32] Around this time, censorship becomes the main strategy for internet governance. Security rationality relies on a discourse of protecting the public from dangerous online content. As criteria for censoring websites reveal, security discourse is

governing the political life in Turkey. It can be argued that with such recourse, Turkish state acts as a technological surveillant state. Such a process targets dissident politics and effects formation of digital counter publics (Çelik, 2015 , p. 257)

[32] Law number 5651 defined the following criteria that would allow the censoring of websites: "obscenity, sexual exploitation of children, promotion of drugs, prostitution and promotion of suicide".

based on a moralistic framework. It is possible to say that "protection of the morals of the public" is the main aim around this time. This first movement is also crucial, for it introduces elements of criminality into internet communication.

The second moment, has come around in 2011. A lot has happened in 2011 for internet governance. A nationwide filter has been introduced, taking the security rationality of law number 5651 further. Announcement of the filter sparked a massive demonstration against internet censorship. Again in 2011, the PARDUS project, which used to accommodate software engineers working on the open source operation system, has been shut down. Linked to the general change of personnel at TUBİTAK, end of PARDUS signified the end of state sponsored open source work, and prioritization of cyber security and cryptology work. I think this second moment matured in 2012, with the establishment of cyber crimes police division. Since its inception cyber crimes police deals of information theft, hacking and fraud incidents. These crimes, as well as the changes in TUBİTAK do not reflect a moralistic approach. I argue that 2011 is the moment of the emergence of a security approach that is based on technical necessities. Object of security is no longer morals of the people, but rather the digital systems and information stored within them.

This moment brings about further criminalization of the Internet; however, this time the subject matter of the criminal action was not circulating content but rather the system security. Discourses and institutional steps taken within this second movement show an increased effort to secure digital systems, especially those used by state institutions. Change from moment one to moment two results in redefining of the risk from "dangerous for public" to "dangerous for database."

Two moments rely on different strategies of power and bring about different governmental possibilities. However, they are not entirely distinct from one another. Strategies of power that they rely on do not have clear-cut boundaries; thus the definition of these two moments depend on a meaningful coherence, rather than a theoretical and practical exclusion.

Morally legitimized censorship of the first moment uses several strategies of power. Espionage is one strategy to ensure continuity of website censorship. Through involvement of individual internet users in the selection of websites that are to be censored, censorship can be defended among actors within the governance field that stand oppose it. Inclusion of internet users into the censorship process brings about another strategy, one that is based on the evaluation of the content that circulates online. Evaluation of online content is distinct from online data processing[33], for it is suited to the needs of conserving a moral order, rather than to the needs of system security.

Cyber security reliance of the second moment uses two central strategies. Initially, it relies on the establishment and use of a police division specializing in cyber crimes. While cyber crimes police engage in police operations against morally defined criminal behavior, their major specialization is infiltration of digital information systems, fraud through digital systems and information theft. In this sense, use of police forces seeks to deter criminals from engaging in criminal conduct, as opposed to censorship, which seeks to cancel out the effects of content online by making them inaccessible. It is important to note that cyber crimes police has also been used in arresting twitter users who have shared information on the dissent.

[33] Data processing is often done by digital applications, that search and catalogue data, where as moralistic evaluation uses humans to determine whether content is morally degenerative or not.

Where deterring is not enough, increasing technical capabilities is eminent to ensure digital system security. Therefore, second moment is based on education and branching out of computer engineers into requirements of information security and systems security. The technical base of cyber security makes technical systems the principle actors of the internet governance. Their conditions become the central topic of security focused internet governance. The object of protection shifts from humans to digital systems, which results in the expansion of a whole field of cyber security.

3.4 Security rationality and legality

Research on cyber security practices in Turkey reveal that laws and other kinds of legal texts are central to many governmental tactics. Laws provide a complicated arrangement that goes beyond the simple prohibited/allowed binary. Since governing can include use of laws as tactics (Foucault, 1991, p. 95), laws are relevant to strategies of power that are at work in cyber security field in Turkey.

Laws, treaties and planning documents serve multiple functions, primary aim of which is the distribution of responsibilities among the actors that contribute to the governing of Internet. They assign institutions, private companies and individuals with such responsibilities that they arrange their conduct so that desired power effects arise.

Most of the legal texts relevant to cyber security have a prohibiting tone and an interfering character. They prohibit ways of conduct, as the field in which they are written is a security focused field, and as definition of criminal behavior is central to the cyber security strategies. They reflect an interfering attitude, such that they put forward a schema in which actors organize their internal and external manners.

It is possible to think of the prohibitive and interfering character of cyber security texts in contrast with several governmental strategies. Prohibition of conduct is primarily a way of constraining exercises of freedom, that which digital telecommunications render possible. Historically, communications technologies have served as instruments of freedom and "technological foundations of a liberal public space" (Barry, 1996). Prohibitive character of cyber security legal documents limits exercises of online freedom. It contributes to transformation of digital communication technologies into a space of control.

Intervention in actors' conduct is, on the other hand, in contrast with the set of assumptions that neoliberal rationality relies on. Neoliberal governing rationality assumes a free actor, which is manifested in free market. Neoliberal rationality assumes actors are capable of attaining skills for their well-being. Those who are not capable are imposed with a responsibility to be so (Rose, 1996). Legal texts in question assume state actors are incapable, and thus require intervention. Although assuming incapacity of actors is contradictory to distributing responsibilities, this is the case in internet governance in Turkey.

While laws aim to shape state actors, private companies and individual citizens are handled in a different manner in legal texts. Self-responsibilization is still at work, albeit in a different way.

Turkish citizens are constantly made aware of risks of being online. Cyber security actors present dangers that digital systems are capable of hiding from internet users. Citizens are made aware of the risks of being online, with the hope that they will act responsibly and provide their own security on the Internet. Self-responsibilization strategy of neoliberal political reason finds its way into security oriented government of Internet in Turkey. In fact, this brand of self-responsibility is a crucial element in the constitution of economic interest structures in cyber security field. Laws are disinterested in citizens and private companies capacity as actors. What it is interested is the formation of a free market of expert services. This way responsibilization is placed within the market logic.

Laws about cyber security show the drastic change from a security-oriented move within the internet governing in Turkey. As they reach out to some actors in a prohibitive and interventionist manner, and some in free market rationality; they leave governmental strategies that encourage empowerment through technology use in secondary position.

While laws and legal texts speak to state actors, civil society organizations, companies and individuals in different ways, total effects of these texts are central to dominance of security rationality in internet governance in Turkey. As we shall see, primary laws that regulate internet services and online behavior push toward securitization. Laws that regulate online affairs are limited in Turkey, and ones that are in use are concerned strictly about possible security breaches. Three legal texts are analyzed in this section. The law number 5651, which is currently the major law that Turkish government bases itself in dealing with internet related problems. Second is the Cyber Crimes Treaty, signed in the European Parliament. This document is important in showing how security rationality is lingering among legal circles in the international arena. And lastly, National Cyber Security Strategy Action Plan document, which lays an outline of steps to be taken in strengthening state owned digital systems against cyber threats.

3.4.1 European Parliament Cyber Crimes Treaty

A broader understanding of cyber crime took hold in legal texts by way of an international treaty. Designed by European Parliament in 2001, Turkey signed Cyber Crimes Treaty in 2010. Signed with some reservations, Turkish parliament passed "(No. 6533) Law for certifying the Cyber Crimes Treaty" in May, 2014.

In the law, several actions have been emphasized in the definition of cyber security. An apparent emphasis is placed on data. Deleting of data is defined as a major crime. In cases of stealing personal data, if the hacker destroys some of the data, the sentence is increased. Additionally, continuity of the act is also emphasized.

System security has a stronger penal emphasis than data. The disruption of a systems working is seen important, especially if the system fails to work after the act takes place. Placing alien data in a system is equally criminal.

A more comprehensive definition is given at the website of Istanbul division of the Cyber Crimes Department. Here cyber crime is defined as: "crimes that target the security of an information system and/or data in said system and/or users present in said systems and committed through the use of information systems. Cyber crimes are distinct from other crimes in that they can not be committed without using information systems. These kinds of crimes are endemic to computers and internet." The website explains cyber crimes further: "According to Cyber Crimes Agreement and to the departments perspectives, cyber crime is, infiltrating in an information system unlawfully, and acts done afterward.” The examples provided on the website are as follows: Harming a system through infiltration, erasing data, cryptography, taking control of systems, adding data, preventing access, intervention in the anonymity of personal life, blocking telecommunications, unauthorized surveillance of telecommunications and recording telecommunications.”

3.4.2 National cyber security strategy document

National Cyber Security Strategy and Action Plan for 2013 – 2014 document signify an attempt by the state in taking a step in securing the digital information infrastructures that state organizations use. It brings about establishment of new institutions, bureaucratic divisions that are authoritative of governing the cyber security.

National Cyber Security Strategy and Action Plan for 2013 – 2014 document was announced on June 20th, 2013 (Turkish Ministry of Transport, Maritime Affairs and Communications, 2013). The following institutions prepared it: undersecretaries of health, transportation and justice ministries, national intelligence agency, and fiscal crimes authority. Officials from these institutions gathered under the title “Cyber Security Board (Siber Güvenlik Kurulu)”. The Ministry of Communications, Maritime and Transportation were the leading authorities in executing the decisions declared by the document.

The document is significant in introducing a new institution as well as establishing a division within government offices. Among the new institutions, the most significant two were National Center for Intervening Cyber Events (Ulusal Siber Olaylara Müdahale Merkezi - USOM) and Cyber Events Intervention Squads (Siber

Olaylara Müdahale Ekipleri - SOME). These two bodies are proposed as the leading institutions working towards the protection of state owned information systems.

According to the document, USOM is designed as a central governing authority regarding cyber security of critical infrastructure and state digital communication network. USOM coordinates SOMEs according to cyber security plan defined by the Cyber Security Board. USOMs also coordinate collaborations with law enforcement agencies when criminal investigation is required.

SOMEs, on the other hand, are found as executing bodies that take action inside various sectors. SOMEs are designed as subdivisions within ministries and institutions where necessary. Working as a part of the institution they are located in, SOMEs are responsible of the cyber security of the institutions in question.

3.5 A Short history of policing cyber crimes

In the security-dominated view of internet governance, technologies of power that seek to protect the individual from the dangers on the internet precede the system security approach. Protection of individuals became a publicized anxiety, which became evident after founding of cyber crimes police force. Securitization of the Internet requires a public perception of danger. Perception of danger was created soon after newly found cyber crimes police started nation wide operations. Operations provided the ruling party, AKP, a leverage to pass law number 5651[34]. In addition to political outcome of passing of the law, founding of cyber crimes police force made a new capacity available for governing of the Internet.

[34] (Babacan, 2006)

The police division responsible for cyber crimes is the Department for Struggle against Cyber Crimes (Siber Suçlarla Mücadele Daire Başkanlığı). Prior to establishment of the department, it was established as a branch (masa) within Financial Crimes Division in 2004, after which has been transformed into a section head (şube müdürlüğü) in 2007 (then was named as Information Systems Crimes Branch Office). Only in 2012 a department has been founded, and the name of the unit has been changed to what it is today. The department is stationed under the Directorate General of Security (Emniyet Genel Müdürlüğü).

Forming of the Information Systems Crimes Branch Office in January 2006 was a crucial step. It was the definitive institutional formation that paved the way for entrusting police forces in dealing with cyber crimes.[35]

Formation of the police force enabled targeting individuals as culprits in cyber crimes. Prior to the formation of the task force, individuals were not held responsible for the content they publish online. Instead, legal process held access provider companies responsible for crime. In cases when individuals shared copyrighted material on a website, the court would hold the company that provide the servers for the functioning of the website responsible. During this time, commercial bodies were the objects of juridical process.

This approach was evident during a serial of complaints that Turkish Phonographic Industry Society (Bağlantılı Hak Sahibi Fonogram Yapımcıları Meslek Birliği - MÜ-YAP) filed against websites that share MP3 music files. In 2005, MÜ-YAP contacted several websites claiming copyright infringement, asking for compensation in 100,000 lira. Following failed attempts for compensation, the issue was taken to

[35] (Nebil 2006b)

prosecutor, who ordered blocking of 154 websites.[36] A similar complaint was made against Ekşi Sözlük website in 2004, which was resolved without blocking after the website removed content that allegedly defamed Adnan Oktar. Following an appeal by Oktar, court has ordered for removal of content. However, following actions of MÜ-YAP, Oktar appealed again, which resulted in blocking of the social network Ekşi Sözlük domain. Blocking order was realized only by TTNET, which back in pre-ADSL days was not the de facto monopoly as it is today. Although Ekşi Sözlük took the issue to the court and lifted the ban[37], MÜ-YAP case served as a precedent decision. Until passing of law number 5651, MÜ-YAP case was used for blocking 1436 websites in two years.[38]

Following the establishment of cyber crimes police, a new method of dealing with cyber criminals appeared. "Prosecutors order blocking of content" method was replaced with police investigations. At the focus of said investigations rest not the websites, but individuals. Role of the police has been defined so that they track individuals on the Internet, figure out details of their unlawful behavior and find their partners in crime, if they have any.

Cyber crimes branch office made its debut by a nationwide operation against individuals that possess child pornography. In late 2006 and early 2007, police operations in several cities have been made.[39] [40] Operations were unprecedented. It was the first time individuals have been arrested for their actions on the Internet. The actions in question were downloading pornographic material including of minors and visiting

[36] (Nebil, 2006a)
[37] (Seçen, 2006)
[38] (Nebil, 2015)
[39] (Milliyet, 2006)
[40] (CNN Türk, 2006)

websites that host pornographic material including minors. Although these cases hit the headlines, cyber crimes polices also targets fraudsters, scammers and commercial burglars.

Child pornography arrests had a broad impact on the public. Government cited cases as to show how internet was a dangerous domain and that state needs to define unlawful behavior within this domain. Law number 5651 was passed in response to the arrests, which forms the basis of all prosecution of crimes occurring on the Internet. Child pornography operations provided the government with ground to insert security concerns in Internet debates. Child pornography operations were the catalyzer for political maneuvers to increase security-based understanding of internet government. Although danger is argued to arise from pedophiles; measures taken, such as restrictions brought upon cyber cafes, indicate that state intervention problematized cyber behaviors of not just a criminal few, but everyone in Turkey.

The impact of child pornography operations did not diminish with the passing of law number 5651. Protecting public from content circulating on the internet became the next great concern. As politicians presented internet as inherently dangerous with reference to police operations, discourse of "responsibility of state to protect public online" intensified. Argument followed that internet has to be filtered in order to protect children from dangers online. In 2011 a two level filter was introduced, affecting all of Internet connection in Turkey.[41] De facto monopoly TTNET introduced filters, which were obligatory, meaning users were forced to select among filters provided. Mass filtering resulted in massive amount of censored websites. Although protection of

[41] (Radikal, 2011)

children was the main argument, it turned out a website publishing educational material on evolution has been censored as well.[42]

It appears that formation of cyber crimes police provided security for individuals separate from criminal individuals on the Internet. The individual has been problematized in government of Internet in the past. As I have argued before, Internet was seen crucial in the development and empowerment of the individual. However, the problem of the individual has not been addressed within the confines of security focused governing strategies. Founding of the police forces allowed security strategies to overcome the problem of the individual by way of redefining individual as source of potential threat. In terms of governing technologies, police forces linked the government process with physical presence of individuals.

3.5.1 Policing as a governmental tool

Targeting individuals for their online behaviors was a new capacity at the disposal of those who govern the Internet in Turkey. Policing proved that online actions are not detached from physical world. One could act on the Internet, and suffer the consequences in reality.

It was part of a process that reflected obsession with securitization of Internet. Policing introduced the individual as a problem of security in the internet governance. Individual was either source of danger, or as one to be kept safe.

Introduction of police forces made new governmental technologies available. Threat of physical violence, which is used as retaliation to cyber acts, is one of them. Police forces become the material manifestation of prohibitive governmental

[42] (Apaydın, 2011)

technologies. And in their specific capacity, they can prohibit in the individual level. A similar prohibitive approach is at work in the form of website blockings.

While police forces can be a tool of governing, the initial function of policing is not to govern things (Foucault, 2007). Police forces investigate, and eventually, incarcerate. Primarily, policing function is that of control[43]. Excessive policing means that one does not govern, but control. However, police forces can still be used as a governing tool on condition that they are used selectively (Mitchell, 1991).

Use of police as a government instrument brings about certain strategies up front, such as creating hierarchies and direct intervention in conduct of persons. Hierarchy between criminal and innocent, prohibited and allowed, is not necessarily compatible with other kinds of governmental strategies. For this reason, as governing aims at achieving ends by working through societal forces, prohibition has a limited use as a governing strategy. While, governing requires a complex arrangement of institutions, knowledge production and applications; policing relies on a different source of legitimacy. It is not the knowledge and the expertise that govern through policing technologies. In fact, Foucault defines police state as one in which government by decree takes hold, marginalizing the distinction with government by law (Gordon, 1999).

This chapter presents the main case for uses of cyber security practices in Turkey. In its short history, cyber security field has flourished to include individual security experts,

[43] Use of police forces points towards a form of power that is better defined as sovereign power, a concept which is distinct from governmentality in Foucault's thought.

companies providing services of systems security, purchasers of security solutions, state institutions and police forces. Law making process has been of central importance, directing the field of cyber security to immediate political interests of the ruling party. Education and redirection of computer engineers into systems security shapes the kind of expert knowledge being produced, resulting in abandonment of expert knowledge unrelated to systems security.

There are two moments in the history of internet security in Turkey. Moralistic approach, which focuses on the protection of internet users, defines risk in moralistic terms and relies on censorship. The moment of cyber security, on the other hand, focuses on the protection of digital systems, and defines risks in technical terms. I argue that the formation and expansion of the field of cyber security provides a crucial strategy of power, that of nullification of unwanted forces of governance. This strategy of power is crucial in the overall government of Internet in Turkey, for it requires increasing of the technical capabilities of governance actors for achieving the aim of securing the Internet.

CHAPTER 4

GOVERNING INTERNET IN TURKEY

The current condition of internet governance in Turkey embraces conflicting practices. At one end stands the massive FATİH project aimed at teaching internet use to high school students and at the other end we have cyber security laws and practices. Between these somewhat conflicting poles, current internet governance finds its shape. In order to make sense of the rise of cyber security concerns, and with it governing-for-security techniques, we have to look at the broader picture.

This chapter aims to provide a broader picture of internet governance in Turkey. Diversity of the discourses and practices show that distinct and at times conflicting technologies of power are at work in internet governance in Turkey. Strategies of power associated with neoliberal rationality are examples, particularly information age discourse[44], empowerment of individuals and emphasis on the responsibility of governing institutions. Other sets of strategies of power follow a disciplining logic that finds its form in practices of surveillance and censorship.

A lengthy discussion of said technologies of power is not possible in the limits of this chapter. Instead, this chapter will locate several spheres in which surveillance and

[44] Ideals of information age discourse are most visible in the FATİH Project. Project seeks to increase internet literacy and expanding the use of internet in schools. FATİH project, which has been in development for years, aims at providing a tablet computer for every student, as well as digital blackboards for classrooms. A similar approach to internet governance, which prioritizes internet literacy, is also apparent in annual Internet Week celebrations.
FATİH project is an essential force in internet governance. It stands in the converging point of increasing individuals' technological capabilities and personal empowerment. It is reflective of governmental concern with individuals' capacity to use technological devices sufficiently (Barry, 2001). It is reflective of a governmental desire that longs for technologically up to date citizens. FATİH project in this sense is a result of a deep trust in the internet as a governmental tool. It is contradictory to governmental practices that view Internet as an inherently uncontrollable, and thus a dangerous field.

empowerment of individual Internet users occur. Fieldwork has shown that practices of censorship and surveillance have far surpassed practices aimed at empowerment of the individual citizen through participation into flows of information.

Empowering potential of Internet has played a crucial role in the early years of internet governance in Turkey. It has provided a framework in which social problems are reevaluated. Empowerment of individuals, which is rooted in the discourse of information age, has claimed citizens empowerment through potential ways internet provides for citizens to participate in the democratic processes. This claim is of central importance to internet governance in Turkey, for consequent rationality of security derives its legitimacy from information age discourse. Without recognition of the empowering potential of Internet, discourses and practices of security would have no popular grounding.

4.1 Current state of internet governance in Turkey

Alternatif Bilişim Derneği, an independent non-governmental organization (NGO) focusing on informatics, publishes annual reports, which provide the current state of the Internet in Turkey. According to these reports, Turkish state is an active actor in controlling various aspects of the Internet (Alternatif Bilişim Derneği, 2013). From ownership of the physical infrastructure to monopolizing the market for providing internet service, state holds on to fundamental requirements to keep Internet under control.

Internet Authority (TİB), an institution serving under the Ministry of Telecommunications, is granted with authority to interfere in internet traffic. TİB censors websites, by blocking access to the specified ones or virtually shutting them off by closing their servers. In many cases, TİB is unmonitored in choosing which websites are to be blocked. Current legal code allows officials at TİB to censor websites first and apply for a court rule afterward.

State makes its strongest appearance in the government of the Internet in Turkey through TİB, which functions as an institution of control and surveillance. TİB does not seek to govern the content that circulates on the Internet, it merely attempts to control and block content when necessary. However, TİB is part of a greater governing strategy, one that utilizes techniques of control within governing strategies. Kinds of deeper surveillance and blocking that TİB is incapable of requires recruitment of private companies. These companies, with specific surveillance products, are hired directly by state institutions, in a way rendering the state as recruiter of third party companies.

Surveillance of internet traffic is a technique used in many cases. TTNET monitors and records all internet traffic that goes through its servers for six months. Additionally, TTNET uses services of the company Phorm, which specializes in monitoring internet traffic of users and displaying advertisements based on user traffic history. Phorm monitors traffic through a particular technique called deep pocket inspection (DPI), which is a more intense form of surveillance, spanning across boundaries of World Wide Web protocols to email protocols and such. Similarly, The General Directorate of Security is revealed to be a customer of Hacking Team, a company specializing in monitoring encrypted[45] data.

[45] Encryption is a method of securing data behind passwords. Encryption secures data by placing it behind a mathematical algorithm that can only be passed if the recipient has the correct passcode. The practice of using mathematical algorithms for encryption is called cryptology.

Hiring of third party companies to perform specific surveillance tasks is in part reflective of the neoliberal rationality at work in internet governance. Instead of accommodating experts within state institutions, free market of experts are called upon. The turn to free market of experts is a crucial element of neoliberal political rationality (Rose, 1996). State based actors of internet governance that rely on the logic of the sovereignty of the state make use of products of online surveillance, sold by third party companies. Products of Phorm and Hacking Team are instrumental to prevention of access to leaked information belonging to state institutions. They are part of a governmental strategy, namely de-statization[46] of expert functions. De-statization occurs at the precise moment when state chooses not to cultivate certain capabilities within itself but to purchase them through free market of experts. Although authority of the experts is not entirely detached from apparatuses of political rule, as Rose argues; a certain de-statization of some key functions occurs.

On the legal level, laws have approached governance in a mainly prohibiting tone. A law of central importance, Law number 5651, is particularly concerned with laying out the criteria for censoring websites. Recent additions to the law aimed at reconfiguration of the blocking process to expedite it. Law does not define in what ways internet service should be provided in order to maximize the public good. Public good and minimum requirements for sustainable internet accessibility are out of the scope of Law number 5651. It is limited to framing criminal behavior and content online. The law number 5651 declares that internet service providers (ISPs) are responsible of recording and storing all user traffic for six months. The data stored is to be handed over to

[46] De-statization refers to the dispersion of practices associated with state institutions in preference for external forces, such as the free market.

security forces if they are required. According to the law, ISPs are to obtain equipment for storing data on their own.

In short, it is possible to say that the government of the Internet is not dominated by a single rationality. Multiplicity of techniques of surveillance and censorship shows a restrictive rationally that holds an upper hand in the government of Internet. However, diverse characters of the actors involved in surveillance and censorship often makes it difficult to talk about a unified governing rationality; just as practices towards increasing internet literacy has little in common with practices of surveillance and censorship.

A dominant theme that appears in various techniques of power is capacity for control. State seeks to increase its control capacity in the matters around the Internet. It seeks to dominate the market for ISPs. It seeks to control the websites, which users in Turkey would want to access. It seeks to be informed about the internet traffic of users, and be in control of the technical infrastructure that enables spying on users. The desire to be in control is apparent, however it is not fulfilled entirely.

In order to achieve a sufficient level of control capacity, state governs various forces existing in the Internet field, constituting new ones when necessary. Failure of one kind of technique can be the legitimizing source of the establishment of other kinds of techniques. Increase in dominance of cyber security practices over various practices of internet governance comply with state intention to increase control capacity of the internet field. The rest of this chapter focuses on various forces within internet governance. State institutions, civil society organizations, laws and technical equipment are listed with reference to their function in internet governance. Cyber security practices sometimes contradict to these forces, sometimes it works with them in harmony. While there is not a unified objective among these actors and forces, these are the forces against which cyber security comes to reflect rationality of security, and particularly the technique of nullification, through its encounters with these forces.

4.1.1 Infrastructure

The physical infrastructure of the Internet in Turkey includes fiber optic cables and routing hardware. These physical materials are the basis the virtual communications takes place. There are two kinds of fiber optic cables, those that are laid on land, and those that are laid on the sea floor. The second kind includes massive cables that enable global communication, connecting national networks with high bandwidth. The land cables are also connected to the networks of neighboring countries. The aquatic fiber optic cables that Turk Telekom is partners of are called SeaMeWe-3, which spans from Northern Europe to East Asia and Australia, MedNautilius, an east Mediterranean cable, KAFOS, west black sea cable and Turcyos that connects Turkey and Cyprus.

TTNET, a subsidiary of semi state owned telecom monopoly Turk Telekom, is the monopoly internet service provider (ISP). Although there are numerous other ISPs, they are dependent on TTNET for the infrastructure. These secondary ISPs, such as Superonline, simply rent bandwidth from TTNET and sell it to third parties. As of 2001, ADSL technology is used in distributing internet service.

State treasury owns 30 percent of TTNETs shares. Ownership of high rate of shares in the monopoly ISP ensures the state a role as an observant in the internal decision making process of the TTNET. As a shareholder, state treasury has the right to observe the way company conserves its profitability. The decisions on the profitability of the company do not have to be in correlation with the interest of the state. The way internet service is provided can have implications on the population[47], which would determine the way in which state acts to the problems arising from the Internet use of individuals. Ownership of TTNET shares provides state officials and politicians with an influence on the direction in which the company applies technologies and services.

TTNET maintains the policy of providing "safe internet" to its customers, which forces users to select among three packages, each filtered with various measures. After mass protests in 2011[48], the company made changes to the package system however, has not changed their implementation. In addition, the "fair use" policy implemented in 2012 enforces a quota system, which reduces users to broadband speed in case the traffic quota is exceeded.

4.1.2 Legislation and internet governance

The passing of law number 5651 marked a crucial step in the internet governance in Turkey. Named, "Law Concerning Regulating Publications on the Internet and Preventing Crimes Concerning These Publications", law number 5651 was unprecedented as a legal document that took Internet as its main subject.

[47] An obvious implication lies in the efficiency of the performance, without which Internet use of an entire nation would be dissatisfying and useless. Additionally on the technical level, ways in which technical properties of the internet network is set up can affect users' internet experience. For example, computers in Qatar (or most of them) share a single IP address. This condition stems from the fact of monopoly ISP in Qatar uses NAT, to modify users network address when they are browsing in international networks. Use of NAT technology to convert all IP addresses from a country makes it easier to control Internet traffic, as is exemplified by Wikipedia's accidental ban on Qatar's single IP address.

[48] In 2011, TTNET announced that its going to impose a nationwide filtering system, in which every internet user would have to choose from specified filters. Filters were to result in mass online censorship. Mass protests were organized in thirty cities, under the shared slogan of "Internetime dokunma" (Hands off my Internet).

As the first comprehensive law to define the role of institutions in internet governance, law number 5651 was very much anticipated by civil society organizations active in the telecommunications field. Demands were for a collective negotiation process that included state institutions, civil society organizations and the private sector. However, as the bill evolved into final draft, police forces organized nationwide criminal operations for ownership of child pornography. These operations were widely used in the media to provide pretext and justification for tighter control of internet traffic by the authorities. Particularly, members of the ruling party put forward arguments for a tighter internet regulation. Under a heavy political pressure and broad criticism from civil society organizations, the law was passed in May 2007. It defined responsible actors and institutions, such as content providers, hosting service providers, and ISP's.

Defining responsible actors is a crucial element for the government. As governing of internet can not be done by a single institution, defining the rules of interaction between institutions, political actors, civil society organizations and private companies is necessary. It is essential, for art of government requires efficiency of powers used in government (Foucault, 1991). While the rules of interaction is fundamental to government, the specific ways in which law number 5651 distributes responsibilities indicate a narrower aspect of government, a neoliberal governing rationality. Neoliberal governing rationality calls for the active involvement of individuals and collectivities in resolving issues of government (Burchell, 1996, p. 29). This brings out involvement in governance. However, to be involved brings with it responsibilities.[49] Individuals publishing content on the Internet, server companies that

[49] As Graham Burchell explains, involvement in the governmental process does not necessarily lead to equal representation of the constituents in governing. Constituents, "must assume active responsibility of

sell server space service and ISP's are made responsible through the law number 5651. Though these actors are involved in the government of internet, they are left on the fringes of the governing techniques, most influential of those, which are occupied by state institutions and monopoly service provider TTNET. Nonetheless, they pay the price of being involved in the governmental process, and conduct themselves in the lines provided by the law (Burchell, 1996).

The rules of conduct that the law puts forward are reflective of the political pressure it was subjected to during its preparation. The political discourse that was used to serve as the justification for the law was based on child pornography. It highlighted circulation of child pornography while keeping silent on other problematic issues. The main argument for the passing of the law relied on the idea that the Internet is a source of danger. Political argument, in which the ruling party relied on, defined danger of the Internet in a moralistic way. The argument was based on unrestrained content circulation on the Internet posing a risk for morality. Ultimately, the law took its shape around the political interest of the ruling party, which became the main catalyst for its passing.

The political pressure for internet regulation did not cease with the passing of the law number 5651. As police operations occurred nationwide, with arrests on child pornography ownership, public support for these operations was used to pass further regulations. Protecting public from content circulating on the Internet became the next great concern. As politicians presented Internet as inherently dangerous using police operations as a reference, discourse of "responsibility of state to protect public online"

these activities, both implementing them and, for their outcomes, in so doing they are required to conduct themselves in accordance with the appropriate (or approved) model of action" (Burchell, 1996, p. 29). As carrying out responsibilities are divorced from defining an approved model of action, constituents of governing process cannot carry their individual interests in the act of governing.

escalated. Argument followed that Internet has to be filtered in order to protect children from the dangers online. In 2011 a two level filter was introduced, affecting all of Internet connection in Turkey.[50] De facto monopoly TTNET introduced filters, which were obligatory, meaning users were forced to select among filters provided. Mass filtering resulted in massive amounts of censored websites. Although protection of children was the main argument, it turned out a website publishing educational material on evolution has been censored as well.[51]

In addition to content in circulation on the Internet, spaces of collective internet access, that is internet cafes, were targeted for further regulation. The anonymity that the cyber cafes provide to their customers was deemed increasingly problematic. After passing of law number 5651, another regulatory document was passed, which brought limitations[52]. Licenses were to be revoked if cyber cafés did not install camera equipment and record the customers' entrance to the facility. An additional filter was mandatory for cyber cafes, which filtered out more websites than the original TTNET filters. Cases of internet filters and cyber cafes exemplify how security outlook in government does not target only the criminals. It targets every internet user.

Developing governing techniques that have an effect on every internet user is a crucial point for observers of internet government in Turkey. Definitions of cyber crimes on which police and the law enforcement act, assume that crimes in question has an individual quality. However, the way these crimes are dealt with enforce strategies that affect every internet user in Turkey. It is possible to develop and employ alternative governing strategies that aim to discipline individual internet users. Strategies of this

[50] (Radikal, 2011)
[51] (Apaydın, 2011)
[52] (Üstündağ, 2007)

kind would involve a preventive approach, aiming to motivate internet users to naturally accept disciplinary norms and values. The reason why this is not the case seems to be related with the increasing of security oriented governing strategies. Governing with the objective of achieving security has strategies of its own. And the case of affecting the population is reminiscent of a fundamental approach in security government. This is because historically, government for security privileges the well-being of the majority of the population, while excluding parts of it from the government. Category for the whole is the category of population. Emergence of the category of population is necessary for dealing with an event that can be a security risk (Foucault, 2007). In fact, for Foucault, category of "population" is crucial in development of government as an art of rule. Governing aims to apply power in the form of economy, and the phenomena within the vast reality codified as population is the object on which the economy of power is exerted.

4.2 TİB and governance

The law number 5651 appointed Telecommunications Authority (TİB) in preventing access to websites defined by the law. The cataloging of websites, deciding which websites fall under the categories defined illegal under the document was a responsibility of TİB. These categories include "obscenity, sexual exploitation of children, promotion of drugs, prostitution and promotion of suicide". While TİB relies on lists made by international organizations in order to filter websites, professionals working at TİB can also add to these lists websites of their choice. This makes them actors in state censorship of websites. Given that the categories defined in the law do not directly refer to absolute conditions, but rather to broad concepts, it is virtually impossible to define the limits within which TİB bureaucrats can censor. It follows from this intended ambiguity in development of the law: officials at TİB can make blocking decisions, even though they do not possess a legal title to do so.

Aside from updating censorship lists, officials at TİB have an other incentive to act as a decisive actor of censorship. In the case of blocking a particular page, a decree from a judge or a prosecutor is required. The judge or the prosecutor warrants the blocking decision and action must be taken within 24 hours. However, in cases when the website that is to be blocked is hosted by servers located outside Turkey, TİB can decide on its own to block access and send the decision to ISP. In such cases, legal decree is applied retrospectively. A decree request is sent to the judge, while access to the site has been already blocked.

These institutional practices are prone to criticisms regarding their legitimacy. However, criticisms do not appear to filter into the governmental practices, and remain irrelevant to those who act. Disregard for legitimate legality appears to be a dominant part of the governing mentality of Internet in Turkey.

Without a legitimizing discourse, and without reference to public well-being, backing up the actions taken over internet traffic becomes problematic from the standpoint of the government. Governing strategies fail to provide the appearance of necessary measures.[53] Instead, they appear to reflect the political interest of the rulers. As government is distinct from direct control, a legitimizing discourse of necessity or

[53] Instead of an inherent necessity of governing process, it is more suitable to talk about the appearance of necessity. Expert knowledge is often built upon, and directed towards a configuration of necessity. As Nikolas Rose explains, political rationality of welfare state rested on a subject of needs, relationships and attitudes (Rose, 1996). Advanced liberal rationality divorces the role of needs in governing, and replaces them with consumer demand, competition and accountability.

accountability must be provided. Experts usually take up the role of providing explanations and authority over the necessity of government decisions. With experts in the field, it becomes viable to argue that a particular decision is within the norm that, with reference to topic at hand, blocking of certain websites is a technical necessity, for the well being of the population[54]. However, as most acts of censorship openly serve the political interest of the ruling party, internet governance fails a fundamental element of governmentality. Principle of "rule without appearing to do so" does not apply in the Turkish case.

It is possible to say that TİB occupies a unique place, among the technologies of power at work in the government of the Internet. It is the central state institution, responsible for maintaining telephone wires and digital surveillance. Although it is often other institutions, such as the police forces or the intelligence agency that provides the will to conduct said acts, TİB is the one institution that capable of wiretapping and surveillance. It is an institution that derives is effectiveness from its capability.

Surveillance occupies a crucial place in Foucault's formulation of disciplinary power. Surveillance, explained through the architectural model of Panopticon, is a technique of power that allows individuals participate in their subjection through visibility of their bodies (Foucault, 1979). In Panopticon, one knows that she/he is seen, but does not know when or by whom. Visibility draws individuals into "a power relation in which he simultaneously play both roles" and therefore shape them as docile subjects (Foucault, 1979).

[54] In advanced liberal rationality, experts are to be divorced from the state. Detaching "authority of expertise from the apparatuses of political rule, relocating experts within a market" (Rose, 1996, p. 41). While some experts of cyber security are located in a competitive market in Turkey, others in state institutions are active contributors of state centric censorship.

In Surveillance Studies, Foucault's formulation of the role and uses of surveillance in production of subjects have been widely influential. However, as the literature expands, Panopticon is not sufficient anymore to explain variety of phenomena. Social media signifies a change in the way individuals' participation of their own surveillance; yet this change is in the opposite direction of the subject of Panopticon, whom relies on the rational calculation of visible conduct. In digital surveillance literature, social media participation puts forward a case for inscribing oneself to surveillance through "faculties of initiative, adventurousness, experimentation, self-assertion, emotionality, pleasure and entertainment seeking" (Bauman & Lyon, 2013, p. 58). On the other hand, surveillance drones signifies different phenomena, where surveillance technologies of surveillance become total and very hard to avoid. In spaces of total surveillance, power results in its opposite, refusal and resistance instead of docility (Rhodes, 2004, as cited in Bauman & Lyon, 2013, p. 54).

In this sense, capability to perform surveillance is a crucial element for the actors of internet governance. TİB's capacity for surveillance is not fixed and is dependent on the cooperation of ISP's and state departments. As explained earlier, this work relies on a concept of government, which revolves around a totality of effects, not an acting center (Miller & Rose, 1992). Laws, institutional structuring, state subsidiary of the market of particular services and outsourcing of software's and hardware acts as an ensemble of forces that affect the way in which internet use takes its current form. The place TİB occupies within this ensemble is that it provides the criteria in which censorship of websites are conducted: the ways in which they are selected and the technologies in which they are censored through. What makes this position unique is that, I argue, it serves as the center in which actors that contribute to the governing of the Internet, translate their interest into the criteria TİB provides.[55]

Within the network in which actions that shape the internet experience, TİB serves as a reference point. Because it symbolizes what the state is capable of, law-making process reflects the capabilities of TİB. Recent addition to law number 5651, which orders for blocking of websites within 4 hours relies on no other than the speed in which experts in TİB can be organized and put into action to run the code to block given website.

Similarly, software developers that sell website filtering software for cyber cafes to use are shaped around the voluntary blockings that TİB officials create. The law requires cyber cafes to run a kind of filtering software. However, because TİB officials often take initiative and block websites, since they can apply for a legal decree later, software developers often add websites to the filter database more aggressively than the law asks them to do so. This is one of the reasons cyber cafes host a more strictly filtered internet service to their customers.

Michel Callon and Bruno Latour ascribe a particular meaning to translation process. According to them, translation allows micro actors to emerge as macro actors: insofar as they are successful to "translate other actors into a single will" (Callon & Latour, 1981, p. 279). While their theorization focuses on how one actor becomes a macro actor, their insistence on concept of will as the unit of which the actor organizes

[55] Miller and Rose explain, with reference to Bruno Latour and Michel Callon (Callon & Latour, 1981), translation as a method in which actors "come to understand their situation according to similar language and logic, to construe their goals and their fate in some ways inextricable, they are assembled into mobile and loosely affiliated networks" (Miller & Rose, 1992, p. 184). In a network in which actors translate from one other, shared interests and common modes of perception arise.

and becomes one with is problematic. Translation of will of the actors in the network is distinct from the practices that support the function of the network in question.

In the Turkish case, TİB serves as the center that provides the main translation reference point. However, this reference point is not composed of, or relies on a kind of will[56]. Instead, in close inspection, the technical necessity for particular software, hardware, expertise and initiative grants TİB this center-like position. It could have been possible to imagine the network in which government of internet is carried in Turkey to be centered around an actor of will, if the particular necessities for security focused governing was not the case. Government for security relies on technological tools that require an assembly of techniques of power, among which setting standards, calculation, repair and keeping up to date are of primary importance (Barry, 2010).

4.2.1 State actors of censorship

An initiative to document blocked websites, Engelliweb[57], has documented that as of December 2013, 35.000 websites have been blocked. All of these websites have been blocked with reference to the law number 5651. An overall estimation by Alternative Informatics Association (Alternatif Bilişim Derneği) regarding the last 6 months of access prevention statistics reveal that roughly 1000 websites are blocked every month.

Telecommunications Authority (TİB) has abandoned publishing statistics regarding access prevention in May 2009. According to Engelliweb, TİB shares the information of blocked websites only with ISP's such as TTNET. Information is not published as a bulk. Upon receiving "acquisition of knowledge" requests regarding

[56] The ruling party maintains the will that organizes the network in which government of Internet takes place. Their short term and long term political interest is apparent in acts of censorship and surveillance.

[57] Civil initiative Engelliweb can be visited at: http://engelliweb.com/

website blockings TİB denied providing information. Binali Yıldırım, who was at the time Minister of Telecommunications, has also denied a response to questions and criticism in the parliament, most of which were voiced out during the parliamentary talks prior to the new additions to law number 5651.

According to the statistics provided by Engelliweb 89 percent of the blockings have been made through administrative decision, meaning TİB has applied for and put into administration the blocking request. For the rest of the blocking decisions, court decree amounts for %5.2 of the cases and prosecutors decree amounts for %2.5.

Loopholes in legal code allows private sector to take action for blocking websites. The law that regulate funding and taxing of lottery grants companies who have the privileges to execute lottery and betting games can take a decision to block other betting websites and send the decision to TİB with no legal ground for objection (Şen 2013).

4.3 Technical aspects of censorship and government

The technical aspects of website censorship pose a challenge for state agencies. These challenges are technical in character, for they cannot be easily overcome by institutional structuring and infrastructural ownership. Even though the physical infrastructure belongs to the semi state controlled ISP, Türk Telekom, the ownership does not directly bring about control of the internet traffic.

There are several technical capabilities state agencies must posses in order to govern the Internet. Among these are recording and storing internet traffic, cataloging and indexing traffic data, blocking traffic on the basis of target IPs, blocking traffic on the basis of target URLs, encrypting potentially vulnerable traffic (of state communications), decrypting traffic deemed dangerous and analyzing deep packet data (DPI). These capabilities are crucial for the state. Technological capabilities are not the only way of increasing control over the Internet. These elements form the material base of internet governance in Turkey. Without decrypting, DPI, URL targeting software and storage servers, internet censorship would not be possible.

State institutions make use of the capabilities outlined above. However, state institutions perform not all of the said actions. Some of them are done "in the house", some given to sub-contractors and some done by private companies under the supervision of state institutions.

The more usual method of blocking websites involves blocking of IPs, done by TİB. The 40,500 websites blocked until a new piece of legislation that passed on the parliament on February 5th 2014 were denied traffic this way. This new law brought some updates to law number 5651, among which were allowing blocking selected URLs instead of the whole hosting website. This sudden legislation was a response to the published sound recordings of then Prime Minister Erdoğan and his son conversing about illegally acquired money. URL based blocking was put to use even before the legislation allowing it has been passed.

During the days the law passed, politicians who argued for the benefit of the legislation said that URL blocking is a more viable option than IP blocking. The argument was that less content would be caught under blocking because instead of entire websites only pages within the websites would be blocked. And this advancement would come to be by means of the legal steps taken by the government. However, IT journalist

Füsun Sarp Nebil argues that the reason for URL blocking not being used is based on a technical obstacle rather than a legal one (Nebil, 2014). Nebil argues that URL blocking brings a great deal of burden on ISPs and consequently internet traffic provided by the ISPs. URL blocking involves technical and administrative workload, for it requires making calculations done within the traffic.

Three methods of blocking websites are used in Turkey: DNS based, IP based and URL based.

DNS based blocking: DNS based blocking relies on the ISPs control of the DNS servers. Because the ISPs control DNS servers, when a user sends a request for an IP address, the DNS servers direct them to a different page, instead of the original IP address. This kind of blocking is easily bypassed by using a DNS server located in a foreign country.

IP based blocking: ISPs use routers. These devices send pockets of data to desired destinations. Routers send data according to the IP addresses. A router checks the IP address and determines which router to send the data to. So a pocket of data jumps across several routers. IP based blocking works when, routers are commanded not to deliver pockets to certain IP addresses. So in this method, when the IP address of a website is blocked, all content within that website is blocked. This was the case when YouTube was blocked. Sometimes same IP addresses are reassigned to a different website. If ISP blocks the IP and does not check if the IP address is assigned to another website that second website is also blocked.

URL based blocking: On the URL based blocking, the DNS server works correctly and the router presents the correct IP address. It works through a piece of hardware installed in the infrastructure of the ISP, which monitors each request for access to IP addresses and sub address. This form of blocking requires surveillance on a greater scale. The data set from which the website to be blocked is much bigger. In IP based blocking, the routers do not look into the content of a pocket, they only look at the IP header and TCP header, similar to that of postman looking at an envelope and not the content of the letter. With URL based blocking however, the content of the pocket must be controlled. Deep Packet Inspection devices do this. The new technical capability required for URL based blocking by being able to look into all units of internet traffic is called Deep Packet Inspection (DPI). Deep packet inspection devices have been present in Turkey. TTNET introduced these devices while promoting "safe internet" in 2011. It was put to use after an agreement with TTNET and Phorm, a digital communications company specializing in the DPI field.[58] Phorm has met criticisms around the world, from activists and politicians alike.

The problem with URL based blocking is that in order to block access to a certain URL, the whole countrywide internet traffic must go through a device. DPI allows for analyzing each individual traffic, so that it is sorted and used against the user.

4.3.1 Role of informants

Law number 5651 did not put emphasis on a policing force. Although coordination with police forces is cited, establishment of related police division was vaguely named in the law. There is also no clear definition as to what should be the role of the police in working with TİB. Even though the law criminalizes certain contents circulating on the Internet, role of the police forces are not clear within the blocking process.

[58] (CNN Türk, 2012)

This ambiguity created a different strategy in locating criminal conduct possible. Because the police was not granted jurisdiction in discovering websites that has unlawful contents, TİB established a website that enabled citizens to report websites that publish unlawful content.

İhbarweb[59] aims to include ordinary citizens in the process of censorship. It calls on citizens to be active agents in monitoring of the Internet and contribute to its control by way of individual efforts. Instead utilizing and relying on a group of experts who would work on censorship İhbarweb relies on the citizens, without an established criteria to rely on while deciding how a website could be harmful. The application interface in İhbarweb website asks users to fill in the reason of application, which is a multiple-choice interface that lists the eight conditions for blocking websites.

The place in which an informant holds in the government of Internet is a particular one. As governance mostly relies on technological devices, of say, blocking access, human informants contribute to governance by taking initiative and defining which websites are harmful for public to see. Their actions, their individual sense of morality affects the way in which internet users experience Internet. I think this is exemplary of the flows of responsibilization[60] through and into governmental practices of security. One can become a part of the governance process however, to do so one should expand the risk in which governance process takes place. Role of the informant is to provide a schema, in which security risk ever expands, thus providing legitimacy for security measures.

[59] İhbarweb is online at the adress: http://www.ihbarweb.org.tr/

[60] Responsibilization is a technique of power, which seeks to make subjects that will voluntarily take responsibilities. Neoliberal political rationality assumes "rational individual will wish to become responsible for the self, for... this will produce... an effective mode of provision for security against risk" (O'Malley,1996, p. 200).

4.4 Access Providers Association

There are various ways institutions can take part in the government of Internet. While institutions such as TİB rely on technical capabilities, others' capabilities rest in their organizational functions. Regardless of their roles in the government of Internet, institutions serve as elements of strategies of power. Institutions act as a force that technologies of power rely on. As mental institutions have served as a major force in the shaping of what regarded as truth about reason and madness, or as prisons have served as centers in which forms of power that aim to shape bodily conduct have been developed (Foucault, 1979, 1988) institutions often reflect the norms on which a strategy of power that they are affiliated with rely on. It is crucial to study the roles governing institutions play in the government of Internet.

Access Providers Association (Erişim Sağlayıcıları Birliği - ESB) is one of such institutions in the government of Internet in Turkey. In Access Providers Association both short-term political interests of the ruling party and the longer-term strategies of security-focused government find their shape. ESB is established by additions to legal code, so that it can direct internet service providers (ISPs) role in internet governance. ESB's primary aim is to increase the efficiency of coordination between state ministries and institutions with ISPs. One of the key matter that requires efficiency of coordination is censorship of YouTube videos and Twitter messages, of the kind state officials have had troubles with after leaks of telephone conversations that reveal media control and corruption. Access Providers Association was founded shortly after the said events, with the objective of blocking online video and sound material within four hours of publishing.

In a sense Access Providers Association is an element among many in the government of the Internet in order to achieve security ends. I find the association a peculiar example of how organizational architectures can make use of the organizational thinking that security government allows. The form that organizational thinking takes is crucial for internet governance, for they can create an organizational background for the government of the technological developments. In this sense, technological developments are not limited to simple artifacts.

Technologies do not operate autonomously: they remain functional only within technological systems (Hughes, 1999). It is possible to see organizational form as a part of the technological system, in that organizational forms have an internal relation with the development of technology (Harvey, 2003). Following the function Access Providers Association serve in the government of the Internet in Turkey, we can say ESB is in an internal relation with the cyber security field.

In the hearth of the process, which result in with Access Providers Association, rests an update to the law number 5651. Passed in February 2014, the new bill redefined the existing law that regulates circulation of content on the Internet. The bill was passed soon after the sound recordings of then Prime Minister Tayyip Erdoğan was published in various accounts throughout social networks. The bill was a response to the inability of state institutions to take down the links that recordings were published. With the new bill, the URL based blocking process was hastened, aiming to prevent the circulation of recordings within four hours.

While technical aspects of hasty URL blocking has been going on in the technical level, an organizational restructuring was needed to speed up the inter-institutional correspondence in the cases of telephone leaks. Essentially Access Providers Association was found in order to speed up the blocking process. Previously, when the court or Prime Minister (in cases of national security) ordered for blocking of defined URLs, the ISPs were informed by personal means, which took part in the technical level of the blocking process. By way of making membership obligatory, ESB functions as a centralized unit that alerts ISPs of their roles in cases of blocking. So it is possible to say that, the primary reason ESB was found is to hasten the censorship process.

The organizational structure of ESB reflects the state dominated objective of the association. By law, ISPs are obliged to join the association. Joining is compulsory for ISPs to keep their operating licenses. Although ESB appears as a civil initiative, Telecommunications Authority (TİB) has founded it by writing the charter of the association. Accounts of the foundation of ESB reveal that only 12 companies have been active in the founding of the association. First general meeting have not been declared publicly, and because of this only major ISPs have joined the association. (Nebil, 2014) An alternative charter prepared by 116 companies has been disregarded in the founding process. It is crucial to note that the semi state owned monopoly service provider Turk Telekom, which has %92 share of the market, dominates the association.[61]

Alongside the political outcomes of the founding of ESB, the organizational structure of the association reflects traces of desire to centralize organizations, which reminds of authoritarian desires. The centralized character of the organization, coupled

[61] (Türk.internet.com, 2014)

with the membership admission process that intentionally leave out many access provider companies, is an example of prioritizing prevention of dissident acts. A centralized organizational model is needed from the standpoint of authoritarian government, in order to censor dissident leaks in a hasty manner. The leaving out of some access provider companies reflects a disregard for the active entrepreneurial subject. Instead of well being of the telecommunication entrepreneur subjects, which complies with biopower, the short-term political interest holds the upper hand, which complies with authoritarian governmentality.

4.5 Blue Coat and outsourcing censorship

State control over the Internet is not self-sufficient in its technological resources. TİB relies on technical experts to conduct surveillance and censorship. While data regarding the conditions of experts in charge of the surveillance equipment are missing from the research at hand, there is an apparent effort to recruit experts who are knowledgeable about technical level of internet communications. Particularly there are efforts in training young professionals to become "white hat hackers", computer security professionals focusing on hacker attacks and system protections. The increase in requirement for security experts is matched by increase in use of hardware and software for facilitating surveillance and control.

Human rights watch group Citizen Lab, founded in Toronto University, conducts research regarding the activities of a US company: Blue Coat. Upon their investigation, activists in Citizen Lab found that there are four companies in Turkey who purchased and are using products by Blue Coat. Four companies are listed in a report Citizen Lab had published (The Citizen Lab, 2013).

Blue Coat produces and sells software designed specifically for nation wide surveillance and censorship. The company was brought to public attention when members of the Syrian digital opposition were tracked down with Blue Coat software and were tortured subsequently. A total of 83 countries are using products by Blue Coat. It is crucial to mention that most of these countries have a bad record of human rights abuses. Turkey is among these countries.

Blue Coat has two products platforms: The ProxySG, providing "SSL inspection" filters unwanted websites and tracks down those who access the websites in question. Packetshaper is a cloud-based network operating software that blocks unwanted traffic.

Turkey is among 56 countries that use Packetshaper. According to Citizen Lab's report, companies Doğan Online, Anadolu Bilişim Hizmetleri, Borusan Telekom, Vodafone and ADSL internet service provider and de facto monopoly of the sector TTNET use Packetshaper.

Keeping in mind that TTNET owns the physical infrastructure of the Internet in Turkey, we can safely say that TTNET has the capacity to block traffic. To what degree this is legal is a highly confusing question. Regulating the Internet is within the authority of TİB, a state institution, which acts and decides legally which websites are to be blocked. Under the law number 5651, ISPs have their own share of responsibilities, which include storing traffic information of its users for six months.

4.6 The PARDUS case and governing computer engineers

Government of Internet includes government of people working in the information technologies sector. A crucial step in the government of experts includes directing expert knowledge to areas that do not allow dissident forms of expertise to flourish.

An example of directing expert knowledge in state sponsored areas is the Fatih Project. Fatih Project aims to provide tablet computers for every high school student in Turkey as well as digital blackboards to classrooms. It is a mass project, and it represents a leap forward in increasing internet access to younger populations. Decisions taken with regards to Fatih Project have had impacts on the IT professionals that form the human resources of any project related to Internet in Turkey.

Use of experts is a crucial element of various strategies of power. Experts often do not stand in direct opposition to political actors, for they are related to political actors in complex ways. Experts, being the technical actors, are active in the shaping of the world and through their knowledge and practice they translate society in an object of government (Barry, Osborne & Rose, 1996). This act of translation does not necessarily fit experts into a schema of interest and functionality determined by politics. Expert knowledge can carry out a function within the framework provided by political rationalities. However, the reverse is also possible. It is possible to talk about a contingent relationship between politicians and experts (Barry, Osborne & Rose, 1996, p. 15). In the Turkish case, a wide number of strategies are employed to keep the relation one sided, for the advantage of the politicians.

Neoliberal political rationality relies particularly on strategies of power in making experts agents of rule. Experts are divorced from the authority of the state, and placed within a free market governed by the rationalities of competition, accountability and consumer demand (Rose, 1996, p. 41). As Nikolas Rose argues, the relation between the state and expertise has been exchanged into one of providers and purchasers. Relation of the experts to individual citizens has been also reduced to that of a service provider.

Government of Internet in Turkey makes use of a free market of computer science experts, to some degree. In matters of providing security services, the expert knowledge has been well commoditized. There are various companies that sell cyber security services for businesses. However, it appears that formation of free market of cyber security experts has occurred as a result of an intervention in the market. Such intervention has been in the form of defunding and canceling out projects, which relies of particular kinds of expert knowledge that can be used in developing dissident technologies. The case of termination of Turkey's major open source operating system serves as the example of such a strategy.

In its initial phase, Fatih Project anticipated reliance to local resources. The actual tablets were to be produced by the local technology firm Vestel, and the software required for running the devices were to be provided by TUBİTAK, the central state institution responsible for scientific and technological developments. The aim was to develop the existing national operating system, PARDUS. PARDUS was an ambitious initiative, for developing a "national" operating system was to provide citizens as well as critical state institutions an alternative against Microsoft's monopoly operating system Windows. An efficient development of PARDUS was crucial for Fatih Project, for it had the capacity to provide a cheaper operating system alternative to be used in tablets and digital blackboards.

PARDUS is an open source operating system; which means its elements are open to anyone to edit and contribute to. At its height, a team of 35 computer scientists was working on the project. However, due to its open source quality, and the additional importance of operating systems in the open source field, PARDUS project was serving as an example of collective software production, which is within the reach of programmers around Turkey. PARDUS functioned as a learning domain, to the young computer scientists who wanted to improve their skills while producing technology. It was in a way, a state investment in software production field in Turkey. It was an intervention in the software market, which would have an immense impact if it were to be actualized. Aside from its market effects, it would contribute greatly to increase of tacit knowledge among the computer scientists in Turkey.

Currently there are only five people working on the PARDUS project. Around 2011, the original team running the project was replaced in a wave of power shift within the TUBİTAK. The latest version of PARDUS was announced in 2013. The operating system was moved to a Debian base, which meant the former developments of PARDUS have been traded with an existing operating system. Reports from open source community revealed that, the new PARDUS was simply branding of an existing operating system with minor additions. With a small crew and the lack of hardware specific software development required for digital blackboards and tablets, Fatih Project is suffering from efficiency problems. Subsequently there have been reports of installation of Windows operating system in digital blackboards.

Coincidentally, around the same time span, there appears an increase in establishment of state institutions and NGOs focusing on cyber security. Can it be a governmental decision to shift focus from production of technology to criminalizing technology? If so it is seeking to find its counterpart in human resources of the field, new graduates of computer science. The increasing discourse of cyber security and cyber warfare, the apparent state support to cyber security NGOs, and institutional incentives regarding system security are pieces in a greater shift in the governmentality in Turkey. It not only seeks to control the internet, but to design the technological field in such a way that, computer scientist, experts, professionals who are responsible of maintaining the software infrastructure of digital communications are kept from developing technology. Instead, as an employment policy, computer scientists are directed to security monitoring jobs, where creativity and initiative is traded off for system maintenance.

4.7 Resistance to centralized governing actors

A method of governing that excludes general public from the decision-making process inevitably produced resistance. While the state approach to Internet governing insists on an empowered centrality, the public opinion, hacktivists[62] and dissident experts call for an end of the centralization politics. Instead a de-centralized and unfiltered Internet without attempts of prying into users data are suggested. State institutions and TTNET, however, do not intend to include general public to governance process.

[62] The term hacktivist denotes hacker activists. Hacktivists use hacker methods, which often include leaking documents, bringing websites down in order to gain political leverage or hacking systems and accounts. While some hacktivists act in accordance with the strict agenda of political movements, most act on the basis of current events, in order to react and protest a high profile event. Almost all, fight against internet censorship and control.

Resistance to current internet government techniques found its form on the Internet and on the streets. A mass protest against obligatory internet filtering was unprecedented, so was the emerging of a Marxist-Leninist hacking collective. Resistance included taking down government websites, leaking secret government information, providing tools for bypassing censorship and distributing tools to crypt communications against surveillance. These forms of resistance do not have a peripheral function in the government of the Internet in Turkey. On the contrary, attempts to crack down resistance are one of the central concerns of internet government. As the state control of the Internet widened, the subsequent resistance was criminalized and the intricate relationship between resistance and control contributed to invention of a new direction for control that is securitization.

Resistance on the streets determined internet filtering as a target. On May 2011, on the eve of voting of the legal draft prepared by Information and Communication Technologies Authority (BTK) a mass protest was organized. The draft included obligatory filters for all internet users, with filters provided by BTK. The four obligatory filters were, "family, child, standard and national" profiles. The announcement of the draft was met with harsh criticism. Among the events that contribute to the mass protest was a leaked email sent to hosting companies from Telecommunications Authority (TİB). The email, which was made public, includes request of closing down of popular websites such as Ekşi Sözlük and Pembe Hayat LGBTI solidarity association. Mass protest marches were organized in thirty cities under the tagline "Internetime Dokunma!" The protests were unprecedented, in mobilizing mass public in a matter focusing on information technologies.

In addition to street demonstrations, resistance to control of the Internet came in the form of hacktivist collectives. Hacktivists did not include themselves at the government process of the Internet. Instead, their strategy was to confront the state institutions directly, by means of taking down sites and leaving messages or warnings. Hacktivism follows a different path than the street demonstrations in this sense. The strategy of convincing state institutions in pluralistic governance has failed. Their strategy was a crucial one, in the wake of aggressive increase of state control of the internet communications, hacktivists aimed at disclosing weaknesses in the states online presence. In addition, the strategy to disclose secret information belonging to state institutions contributed to leveling out the unevenness of transparency between state institutions and citizens.

Among the hacking collectives in Turkey, Redhack remains the most prominent. Found in 1997, the group functions with 12 core members. They have a wide range of operations, including attacking and taking down government websites, cracking databases of police forces, CCTV system, Turkish State Railways, Land Force Command and Ministry of Foreign Affairs. Following the infiltration to the said organizations Redhack leaked documents consisting information of officials. The effect of these leaks was not contained in the cyber space, as the group used the acquired data to put pressure on the government, in cases of social justice and workers rights. In the aftermath of the bombed attack in the Reyhanlı province of Hatay, which took the lives of 52 citizens, Redhack published documents about the attack prepared by the Gendarmerie Intelligence Department. The documents, written prior to the attack, mentioned a bomb attack preparation by Al-Qaeda affiliated rebel groups in Syria. The documents confronted the official argument, which pointed to local cell acting under the directive of the Syrian intelligence agency. Redhack is seen by the government as a terrorist organization, the only hacking collective around to world to be declared so.

Actions of Redhack affect the government process of the Internet in a crucial way. Redhack shows the limits of the states control capacity of the Internet. Regardless of the law making and technological subcontractors to facilitate online surveillance, Turkish state is limited in its online capacities. While website censorship and surveillance of the internet traffic can be done, the overall internet presence of the government is very fragile. Redhack, by preventing access to government websites through DDOS attacks, makes this fragility visible. Government officials in charge of the government of the Internet are aware of this fact. The fieldwork shows that strengthening digital systems is a major concern for telecommunications officials.

Ufuk Eriş argues that hacktivism of Redhack should be evaluated within the framework of new social movements. By categorically differing from revolutionary movements, new social movements aim for the constant disruption of power. According to Eriş, the aim of Redhack is "to show people that power of the rulers is not unbreakable" (Gökdemir, 2013, p. 22). The strategy of revealing the weaknesses of the state on the Internet has found a massive audience. The disclosures of the states weaknesses, paved the way for active involvement of the technical community in the internet government related issues. The power of the expert opinion is not sided with the state in internet government discussions. Often, dissident telecommunications experts confront state legislation and institutions.

Disclosures of state weakness on the Internet have had a major impact on the part of the government officials as well. The message of Redhack's infiltrations of state databases and DDOS attacks has found its response among the government officials. In public organizations, officials often voice out their concerns regarding system weaknesses of state institutions. Additionally by means of Cyber Security Strategy Action Plan state institutions were called for to improve their passwords and to strengthen their protections. Disclosure of weaknesses has contributed to internet government officials' anxieties about system protection. These anxieties found their audience in cyber security and cyber warfare experts, with increasing state support to cyber security policies. In this sense, protection from hackers became a major topic in the internet government circles. And it is the argument of this thesis that cyber security policies provide a new field to internet governance, in which state control is done in the name of system protection.

While, this new direction of internet governance obsessed with cyber security took a lift, civil society is resisting against the government of internet altogether. Alternative Informatics Association (Alternatif Bilişim Derneği - ABD) follows a path of resistance that involves rendering the Internet ungovernable. ABD is active in the political field, as an association of informatics experts. The association is highly critical of the current government strategies. Their "Report on the Condition of Internet in Turkey" is a significant document. Published annually, report brings together actions against internet freedom in Turkey. Additionally, ABD organized an alternative event to Internet Governance Forum (IGF) that took place in İstanbul in the summer of 2014. While IGF acts as a platform to grant current global internet governance model legitimacy, the alternative event called Ungovernance Forum, publicized desires for the complete freedom of the Internet. Discussions on the IGF are primarily concerned with inclusion of institutions to the governance process. Ungovernance Forum, on the other hand provided an arena for discussions that center internet users' freedom online. The event attracted international audiences, and served as a statement against the current condition of the global internet governance in the wake of proof of massive NSA surveillance.

ABD's strategy is not limited to speaking out against internet government. ABD provides cryptography tools, recommendations for VPN services (used to access censored webpages), secure browsers and email clients. ABD initiated "Authorized Eyes Only (Kem Gözlere Şiş)" project that included the aforementioned technical tools for the use of ordinary internet users. These tools, in a technical way, render the government of the Internet obsolete. While providing users means access to censored websites, the project also informs users so they may self-protect on the Internet. The self-protection includes protection from state censorship and surveillance, social web companies and global research engines.

This chapter provides an account of the actors of internet government in Turkey. As institutions, strategies and technological tools are listed, these are presented with their particular contribution to escalation of security rationality in government of internet. Actors are listed with reference to theoretical discussions relating to the functions and roles said actors play in the governance process. Non-human actors, such as technological infrastructure and tools have been introduced, with emphasis on the capabilities or limitations they introduce to the field.

One of the primary characteristics of the field of internet governance in Turkey is that, state institutions act consistently for increasing their capacity to control segments of the field. TİB facilitates surveillance and censorship, and Access Providers Association, although independent on paper, coordinates state and non-state actors in censorship process. Preparation and passing of laws back these state actors and their actions. Thus appears the primary characteristic of internet governance in Turkey: Governing of the Internet in Turkey does not comply with the idea that art of government entails "ruling without appearing to do so".

CHAPTER 5

CONCLUSION

If we are to say the current political state in Turkey is composed of forces and tensions of varying character, cyber security is without a doubt one of them. Daily political debate often include mention of cyber security, with explanations on technical probabilities finding their way into these debates. This is exemplary of one significant element of the field in which this thesis studies: cyber security field is expanding. Increased demand from private sector is matched by the reliance of government officials in their political discourse on cyber security. Looking at the mentions of cyber security, one can see that cyber security is used in debates covering a variety of topics. Cyber security finds its way into political debates about corruption, government takeover, diminishing freedoms, responsibilities of the state and so on.

In the last 3 years, one of the major topics of political debate in Turkey involve conversations of ex-prime minister and several ministers caught in wiretappings. As questions regarding legitimacy of said politicians are still a major element of political life, government officials who defend ex-prime minister use cyber security discourse in countering opposing arguments. Peculiarly, cyber security has become a staple of Turkish political arena through arguments that define wiretappings as violation of the protection of personal information. Internet being the medium in which sound recordings are published, "need to secure" Internet has become a core argument of high profile government officials. In addition, with the increasing use of social networks as an alternative to centralized and government controlled news media, government officials called for securing internet in order to increase capacity of state institutions to control information flows within social networks.

While the release of wiretappings and use of social networks is not the object of digital systems' security, these two elements are crucial in the formation of establishment of internet security practices, which finds its most coherent shape in cyber security practices and institutions.

I argue several points in this thesis:

Firstly, security rationality is becoming a dominant element in governing of Internet in Turkey. Security rationality manifests itself in various ways. Most visible of these ways is the discourse of danger. Experts, politicians and users portray Internet as a space of threat. 15 years ago, a different discourse was present. Discourse of information age, which took development and self-development of individuals through internet literacy as the dominant framework, would identify problems and opportunities internet poses to society as the major political issue. There was a more optimistic sense of the things Internet could offer to society. In the international arena this optimism coincided with the dot.com bubble of the 90's.

Dominance of security rationality is not limited to discursive shifts. Main research agenda of this thesis is to document practices that account for the dominance of security rationality. As I have documented in the fourth chapter, these practices include law making, importing technology, technological outsourcing and establishment of centralizing institutions. These practices are distinct from one another and they are performed in distinct fields of action. While law making is rooted in the political competition of parliamentary politics, law-making process include workshops that bring political actors, state institutions, and non-governmental organizations, chambers of professions. Various actors of telecommunications field participate in the law making process, though sometimes their efforts are left out by the last minute changing of the texts of the law in question. Regardless, participation of multiple actors in the law making process expands number of actors that partake in the governmental practices that find their form in legal texts.

Importing of technology is a peculiar component of security rationality active in government of Internet. As some technological functions require relatively higher levels of complexity, such as traffic surveillance and intervention, several companies that specialize in nationwide surveillance and deep packet inspection find buyers in Turkey for their products. Without strong security concerns, said products would not find buyers. Availability of said products indicate a surge in the security focused problematizing and solution making in global scale.

Establishing of new institutions occupies a greater role in the increased dominance of security rationality in government of Internet. Be it centralizing institutions, or expansion of the police institutions, institutional reconstruction appears as the dominant way in which security rationality is expressed.

All of these, this thesis argues, can be framed as techniques and strategies of power, which represent a rationality that is a distinct form of art of government. Act of governing does not necessarily call for maximization of security. If the political present of the internet governance relies heavily on security practices, this is because strategies and techniques that are distinctively functional for security purposes have been implemented in the recent years in Turkey. Techniques and strategies of security are relied on more then ever, and the way in which technical experts identify and frame problems about internet communications is dominated by security concerns.

Secondly, I argue that cyber security functions as the major field that represents techniques and strategies that are an extension of security rationality. Cyber security practices are capable of representing security rationality dominant in the internet governance circles, due to following reasons: Cyber security field is located within the general field of internet governance. It is a field chiefly occupied by software engineers, most of which are exposed to general changes of policy in internet governance. There is little use of experts that has interdisciplinary qualifications. Actors of cyber security are only concerned with digital systems. Lack of experts and actors that use, say, humanities approach narrow the limits of cyber security field so that it does not extend that of internet governance.

Developments in the cyber security field are not neutral, in the sense that they are not immune to relations of political interest and control. Relative haste of the development of cyber security field is particularly indicative of political interest. As I have noted, cyber security field has been in rapid expansion since 2011. Given the relatively short lifespan of the field, it enjoys a saturated political support, as exemplified by the surge in related law making. However, it is not simply a tool for increasing state control of the Internet, as my conviction in the beginning phases of this thesis led me to think. There is legitimate necessity for protection of digitized personal information, digital systems of critical infrastructures and infrastructure of the local domain name systems (DNS). In the recent past we have seen, leaking of mass personal information database, dysfunctions in electric grid or disconnection of local .tr domain name websites. These events represent a crisis in public security, which politically charged practices of cyber security cannot fully prevent.

I think it is important to note that cyber security does indeed represent a comprehensive rationality, rather than an eclectic totality of practices. Division between the two approaches to security becomes more apparent when we pose the distinction between practices of Internet related security, post and pre 2011. From 2006 on, I have argued, we see the first signs of increasing security concern. These concerns are based on moralistic terms that are elaborated comprehensively. Vague terms such as "morality of the nation" stand out as the major arguments. This changes from 2011 onward, with reference to technical level rather than the moralistic increases in political discourse as well as laws, practices and institutional restructuring. Due to the necessary conviction of cyber security field to repairing and reworking the technical infrastructure of digital systems, its practices are grounded in technical processes. I argue that this grants cyber security field unique techniques and strategies of power. The fact that cyber security field is built upon concrete specifications and necessities of Internet digital information systems technology, they are more responsive to security-focused practices. Because cyber security practices are rooted in concrete necessities, they can be used to nullify actions and agents that share the same concrete ground.

Thirdly, expansion of the cyber security is not isolated to Turkey. There is an ever-growing field of discussion and action on cyber security on the global scale. Shift in global currents in internet governance, state institutions' desire to protect the information held in digital systems and pressures of private sector contribute to these practices. In recent years, several developed countries have started transferring funds and resources into cyber security research and practices. Cyber security divisions are established within armies around the world. Cyber security has grown out a global market for software and hardware for securing digital systems. As I have argued, these products serve a crucial function and contribute to expansion of the field. Although international currents contribute to Turkish case of cyber security, local has distinct characteristics compared to the global. I argue that cyber security in Turkey is primarily a response to the limits of earlier local frameworks of internet security. Prior to cyber security, the major framework of internet security was based on a moralistic discourse, that of protecting the "morals of the nation". Limit of moralistic framework is that its only applicable when public support is sought after. Public support has been used in establishing elementary security practices on government of the internet, say founding of cyber security police forces, however, full potential of these practices requires a shift towards a technical approach to internet security, an approach embodied in cyber security practices.

Lastly, regardless of the specific role it plays in transformation of the way in which Internet is governed in Turkey, cyber security field is still in development. It is not a matured, closed and fully functioning field. The field has not acquired sufficient force of influence, according to experts, in making general public aware of importance of cyber security. For this reason, education is often cited to be a major objective in the field. Cyber security field is still not totally capable of protecting digital systems. However, this is simultaneously a chance to transform the internet governance field. Issues, such as METU and .com.tr, are directed to institutions that are preferred to be replaced by those in power.

This thesis would best serve as an introduction to further studies of cyber security. At the time I conducted the research for this thesis, there was very limited interest in cyber security from social sciences. Lack of published research on cyber security will hopefully change, for I think it is a crucial field that shapes the political status quo.

As a way of closing the gap between social science approach and cyber security field, this thesis focused mostly on defining cyber security, the field in which it is located and the way it is linked to the greater field of internet governance in Turkey. Documenting the present phenomena in a meaningful and coherent narrative was the priority in this thesis. Although the thesis has a critical outlook towards cyber security, it could not evolve into a study of critical subjectivities in relation to cyber security. Although forms of resistance are present in the fourth chapter, issues of resistance and subjectivity could have occupied a greater place in this thesis. Scarcity of sociological study of cyber security in Turkey has led me to prioritize defining the field and laying out central sociological conceptual processes and contradictions. Having this thesis laying out basic processes of the field of cyber security will be instrumental for further studies of dissident subjectivities within Internet as a space of security.

Due to many obstacles, this thesis presents a missing account of cyber security practices in Turkey. Obstacles arise mostly from the opaque character of general workings of cyber security field. Cyber security and internet governance institutions lack a comprehensive account of their daily workings, data of their funding and the technical aspects of their work. While some institutions, most importantly TİB, host a Q&A section on their website, it is far from being sufficient. Most of the technical aspect of internet governance remains unknown even to computer engineers and experts of the field. General public learn about governance decisions from when an independent expert revels them. It has been a crucial obstacle for this research.

Obstacles were not limited to those cyber security field impose on researchers. Some of the obstacles had personal roots. The fact that I do not have a background in computer engineering, coding and an occupational grasp of workings of internet infrastructure in Turkey has limited my research. Research has used accounts of experts and their understanding of the practices they do. However, my approach to these accounts failed to include a critical filtering, for I had to take experts' word on technical level of their work as they were. My lack of understanding of technical workings of cyber security has limited me methodologically as well. Interviews I have conducted failed to grasp the technical level, and my observation in the events I have participated in remained limited. It is one of the reasons why the research for this thesis relies heavily on newspaper articles and published material.

I am inclined to shape the future trajectory of this research in a way that can combine critical security studies with social shaping of technology literature. In its current form, this thesis does not rely on critical security studies. Its primary aim being the identification elements of security rationality in internet governance, it did not focus on general issues within security studies and developing a critical approach to problems posed. Given the importance of internet security debates within internet governance circles, a security focused study of communications technologies will be much needed in the future. I think it is important to produce knowledge about the emerging field of cyber security, from the standpoint of social sciences, so that we can better understand how it shapes internet materially. It is my personal conviction that security is a hyper inflated concern in contemporary societies, and a study of how concern spreads across domains of social life is called for.

REFERENCES

Akdeniz, Y. & Altıparmak, K. (2008). *Internet: Restricted access: A critical assessment of internet content regulation and censorship in Turkey*. Ankara, Turkey: İmaj Yayınevi.

Allen, M. T. & Hecht, G. (2001). Authority, Political Machines, and Technology's History. In M. T. Allen & G. Hecht (Eds.) *Technologies of power: Essays in honor of Thomas Parke Hughes and Agatha Chipley Hughes*. (pp. 1-24). Cambridge, Mass: MIT Press.

Alternatif Bilişim Derneği (2013) *Rapor: Türkiye'de internetin durumu 2013*. İstanbul: Alternatif Bilişim Derneği.

Althusser, L. & Balibar, E. (1970) *Reading capital*. London, England: New Left Books.

Altintas, K., Aydın, T. & Akman, V. (2002). Censoring the Internet: The situation in Turkey. *First Monday*. 7(6). Retrieved from: http://journals.uic.edu/ojs/index.php/fm/article/view/962/883

Anadolu Ajansı. (2016, March 24). Kişisel verilerin korunması kanunu yasalaştı. *NTV televizyonu*. Retrieved from www.ntv.com.tr

Apaydın, B. (2011, December 9). Evrim teorisi 22 kasım filtrelerine takıldı. *sosyalmedya.co*. Retrieved from http://sosyalmedya.co

Aydin, C. H. (2001). Uses of the Internet in Turkey. *Educational Technology Research and Development*, 49(4): 120-123.

Babacan, N. (2006, December 22) Çocuk pornosuna dokunan yanacak. *Hürriyet gazetesi. Retrieved from:* http://www.hurriyet.com.tr/

Barlow, J. P. (1996). A declaration of the independence of cyberspace. *Electronic Frontier Foundation*. Available at: https://projects.eff.org/~barlow/Declaration-Final.html

Barnard-Wills, D. & Ashenden, D. (2012). Securing virtual space: Cyber war, cyber terror, and risk. *Space and Culture*, 15(2), 110–123.

Barry, A. (2001). *Political machines: Governing a technological society*. Cornwall: Atholone Press.

Barry, A (1996). Lines of Communication and Spaces of Rule. In A. Barry, T. Osborne, N. Rose (Eds.) *Foucault and political reason: Liberalism, neo-liberalism, and rationalities of government*. (pp. 123-142). Chicago, IL: University of Chicago Press.

Barry, A., Osborne, T. & Rose, N. (1996). Introduction. In A. Barry, T. Osborne, N. Rose (Eds.). *Foucault and political reason: Liberalism, neo-liberalism, and rationalities of government.* (pp. 1-18). Chicago, IL: University of Chicago Press.

Bauman, Z. & Lyon, D. (2013). *Liquid surveillance: A conversation.* Cambridge: Polity Press

Beck, U. (1992). *Risk society: Towards a new modernity.* London: Sage Publications

Burchell, G. (1996). Liberal government and techniques of the self. In A. Barry, T. Osborne, N. Rose (Eds.). *Foucault and political reason: Liberalism, neo-liberalism, and rationalities of government.* (pp. 19-36). Chicago, IL: University of Chicago Press.

Brito, J., & Watkins, T. (2011). Loving the cyber bomb?: The dangers of threat inflation in cyber security policy. *Harvard National Security Journal.* 3(1). 39-84.

Callon, M. & Latour, B. (1981). Unscrewing the big leviathan: How actors macro-structure reality and how sociologists help them to do so. In K. Knorr-Cetina & A. V. Cicourel, (Eds.). *Advances in social theory and methodology: Towards an integration of micro- and macro-sociologies.* (pp: 277-303) Boston: Routledge & Kegan Paul.

Cavanaugh, A. (2007). *Sociology in the age of the Internet.* Maidenhead : McGraw Hill/Open University Press.

Castel, R. (1991). From dangerousness to risk. In G. Burchell, C. Gordon, P. Miller (Eds.). *The Foucault Effect: Studies in Governmentality.* (pp. 281-298) Hemel Hempstead, England: Hervester Wheatsheaf

Castells, M. (2002). *The internet galaxy: Reflections on the Internet, business, and society.* Oxford, England: Oxford University Press.

CNN Türk. (2006, December 28). 7 ilde porno operasyonu: 3 tutuklama. *CNN Türk.* Retrieved from: http://www.cnnturk.com

CNN Türk. (2012, September 12). İnternet kullanıcılarını bekleyen büyük tehlike. *CNN Türk.* Retrieved from: http://www.cnnturk.com

Çelik, B. (2015) The Politics of the digital technoscape in Turkey: Surveillance and resistance of Kurds. In B. Akdenizli (Ed.). *Digital Transformations in Turkey.* London: Lexington Books.

Dean, M. (2001). *Governmentality: Power and rule in modern society.* London, England: Sage Publications.

Dunn Cavelty, M. (2012). Militarizing cyberspace: Why less may be better. In C. Czosseck, R. Ottis, & K. Ziolkowski (Eds.). *Proceedings of the 4th International Conference on Cyber Conflict.* (pp. 141–153). Tallinn: CCD COE Publications.

Dunn Cavelty, M. (2014). Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities. *Science and Engineering Ethics.* 20(3). 701-715.

Dyer-Witheford, N. (1999). *Cybermarx: Cycles and circuits of struggle in high-technology capitalism.* Urbana and Chicago, IL: Illinois University Press.

Emre, B. (2012a) Siber güvenlikte ofansif yaklaşımlar. Presented at Siber Güvenlik Konferansı. Conference, Ankara, Turkey. Retrieved from: http://www.slideshare.net/siberguvenlik/sgk-sgoy-emre

Emre, B. (December, 2012b) Siber güvenlik – başlangıç. [Web log post] Retrieved from: http://www.siberguvenlik.org.tr/2012/12/siber-savaslar-baslangc.html

Eskicumali, A. (2010). The effects of internet cafes on social change in Turkey: The case of Hendek. *Turkish Online Journal of Educational Technology*, 9(2), 196-204.

Foucault, M. (1991). Governmentality. In G. Burchell, C. Gordon, P. Miller. (Eds.). *The Foucault effect: Studies in governmentality.* (pp. 87-104). Hemel Hempstead, England: Hervester Wheatsheaf.

Foucault, M. (1990). *History of sexuality, volume one: An introduction.* New York: Penguin Books.

Foucault, M. (1979). *Discipline and punish: The birth of the prison.* New York: Vintage Books.

Foucault, M. (1988). *Madness and civilization: A history of insanity in the age of reason.* New York: Vintage Books.

Foucault, M. (2007). *Security, territory, population: Lectures at the Collage De France, 1977-1978.* Hampshire: Pelgrave Macmillan.

Friedman, T. (2005) *The World is flat: A brief history of the twenty-first century.* New York: Farrar, Straus & Giroux.

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

Gordon, C. (1991). Governmental rationality: An introduction. In G. Burchell, C. Gordon, P. Miller. (Eds.). *The Foucault effect: Studies in governmentality.* (pp. 1-54). Hemel Hempstead, England: Hervester Wheatsheaf.

Gorkemli, S. (2012). "Coming out of the Internet": Lesbian and gay activism and the Internet as a "digital closet" in Turkey. *Journal of Middle East Women's Studies.* 8(3), 63-88. Duke University Press.

Gökdemir, O. (2013). *Redhack: Kızıl hackerlar, sanal alemin klavyeli asileri*. İstanbul: Destek Yayınları.

Gürol, M. & Sevindik, T. (2006). Profile of internet café users in Turkey. *Telematics and Informatics*. 24(1), 59–68.

Harvey, D. (2003) The fetish of technology: Causes and consequences. *Macalester International*, 13(7). 3-30.

Hibevefonlar. (2016, February 23). TÜBİTAK-ARDEB Bilgi Güvenliği Çağrı Programı "1003-BIT-BGUV-2016-1 Siber Güvenlik". *AB Hibeleri / Kalkınma Ajansı Fonları*. Retrieved from www.hibevefonlar.com

Hoşgör, Ş. (2013, March 3). Devletten korsanlara 'hacker'lı önlem!. *Vatan gazetesi. Retrieved from: www.gazetevatan.com*

Hughes, T. P. (1999). Edison and electric light. In D. Mackenzie, J. Wajcman. (Eds.) *Social Shaping of Technology*. (pp. 50-63) New York: Open University Press.

Hürriyet. (2012, April, 21). RedHack içişleri sitesini hackledi. *Hürriyet gazetesi*. Retrieved from www.hurriyet.com.tr

Innis, H. (1986). *Empire and Communications*. Victoria and Toronto: Press Porceptic.

Jamart, A. C. (2014). Internet freedom and the constitutionalization of internet governance. In R. Radu, J. Chenou, & R. H. Weber. (Eds.). *The evolution of global internet governance: Principles and policies in the making*. (pp. 57-78). Berlin: Springer.

Karabag, S. F., & Coskun, B. B. (2013). I click, therefore I am: The Internet and the political participation of young people in Turkey. *Turkish Journal of Politics*. 4(1). 113-131.

Karakus, T., Çagiltay, K., Kasikci, D., Kursun, E., & Ogan, C. (2014). Internet habits and safe internet use of children in Turkey and Europe. *Egitim Ve Bilim*, 39(171). 230-243.

Kavlak, O., Atan Ş. Ü., Güleç, D., Öztürk, R. & Atay, N. (2012). Pregnant women's use of the Internet in relation to their pregnancy in İzmir, Turkey. *Informatics for Health and Social Care*. 37(4). 253-263.

Kuzuloğlu, S. (2012, October 16). Nedir bu Phorm meselesi? *Radikal gazetesi*. Retrieved from www.radikal.com.tr

Kus. (2014, June 8). Netclean ve URL tabanlı engelleme [Web log post]. Retrieved from https://network23.org/kame/2014/06/08/netclean-ve-url-tabanli-engelleme/

Leigh, D. (2010, November 28). US embassy cables leak sparks global diplomatic crisis. *The Guardian*. Retrieved from http://www.theguardian.com/

Marx, K. (1990). *Capital: A critique of political economy*. New York: Penguin Books.

McLuhan, M. (1964). *Understanding media: The extensions of man*. New York: McGraw-Hill.

McLuhan, M. & Fiore, Q. (1967). *The medium is the massage: An inventory of effects*. New York: Bantam Books.

Miller, P. & Rose, N. (1992). Political power beyond the state: Problematics of government. *The British Journal of Sociology*. 43(2). 173-205.

Milliyet. (2006, December 26). Çocuk pornosuna üç tutuklama. *Milliyet gazetesi*. Retrieved from: http://www.milliyet.com.tr

Mitchell, T. (1991). *Colonizing Egypt*. Berkeley: University of California Press.

Morozov, E. (2011). *The net delusion : The dark side of internet freedom*. New York: Public Afairs.

Mueller, M. & Wagner, B. (2014). Finding a formula for Brazil: Representation and legitimacy in internet governance. *Internet Policy Observatory Working Paper Series*. University of Pennsylvania, Annenberg School.

Mueller, M. (2002). *Ruling the root: Internet governance and the taming of cyberspace*. Cambridge, Mass.: MIT Press.

Mueller, M. (2010). *Networks and states: The global politics of internet governance*. Cambridge, Mass.: MIT Press.

Mungo, P. & Clough, B. (1993). *Approaching zero: The extraordinary underworld of hackers, phreakers, virus writers, and keyboard criminals*. New York: Random House.

Musiani, F. (2013). Network architecture as internet governance. *Internet Policy Review*. 2(4). DOI: 10.14763/2013.4.208

Mythen, G. (2004). *Ulrich Beck: A critical introduction to risk society*. London: Pluto Press

Nakashima, E. & Warrick, J. (2012, June 2). Stuxnet was work of U.S. and Israeli experts, officials say. *Washington Post*. Retrieved from https://www.washingtonpost.com

National Science Foundation. (2015, October 7). NSF awards $74.5 million to support interdisciplinary cyber security research. *Press Release 15-126*. Retireved from www.nsf.gov

Nebil, F. S. (2014). Beklenen gelişme kapımızda.. Seçimler öncesinde videolar uçuşmağa başlayınca URL bloklama başladı [web log post]. *Yeni Medya.* Retrieved from: http://yenimedya.wordpress.com/2014/01/12/beklenen-gelisme-kapimizda-secimler-oncesinde-videolar-ucusmaga-baslayinca-url-bloklama-basladi/

Nebil, F. S. (2014, July 6). İnternet Erişim Sağlayıcıları Birliği konusunda son durum. *turk-internet.com.* Retrieved from: http://www.turk-internet.com/portal/yazigoster.php?yaziid=47119

Nebil, Füsun. (2015, March 29). TİB neden kuruldu? Müyap engellemelerinden site kapatmalara giden süreç nasıl işledi?. *T24 Bağımsız İnternet Gazetesi.* Retrieved from: http://t24.com.tr

Nebil, Füsun. (2006a, January 23). Müyap; şimdiye kadar 154 site için karar alındı. Tür*k.internet.com.* Retrieved from: http://www.turk-internet.com

Nebil, Füsun. (2006b, June 26). Bilişim suçlarına asayişçi bilişim polisleri-1. *Türk.internet.com.* Retrieved from: http://www.turk-internet.com

NTV. (2013, October 3). İran siber savaş komutanı öldürüldü. *NTV televizyonu.* Retrieved from: http://www.ntv.com.tr/

O'Malley, P. (1996). Risk and responsibility. In A. Barry, T. Osborne, N. Rose (Eds.). *Foucault and political reason: Liberalism, neo-liberalism, and rationalities of government.* (pp. 189-208). Chicago, IL: University of Chicago Press.

Ozgit, A. & Cagiltay, K. (1996). *Türkiye'de İnternet: Dünü, bugünü, yarını* [Unpublished Report]. ODTU-BİDB.

Ozkan, S. & Karabacak, B. (2010). Collaborative risk method for information security management practices: A case context within Turkey. *International Journal of Information Management.* 30(6). 567-572.

Ozmutlu, S., Ozmutlu H. C., & Spink, A. (2008). Internet/computer addiction among juveniles in Turkey. *Proceedings of the American Society for Information Science and Technology.* 44(1). 1-12.

Radikal. (2011, November 22) Filtreli internet bugün başlıyor. *Radikal gazetesi.* Retrieved from: http://www.radikal.com.tr

Radu, R., Chenou, J. & Weber, R. H. (Eds.) (2014). *The evolution of global internet governance: Principles and policies in the making.* Berlin: Springer.

Rattray, G. (2001). *Strategic warfare in cyberspace.* Cambridge, MA: MIT Press.

Rhodes, L. (2004). Total confinement: Madness and reason in the maximum security prison. Berkeley: University of California Press.

Rose, N. (1999). *Powers of freedom: Reframing political thought*. Cambridge: Cambridge University Press.

Rose, N. (1996). Governing "advanced" liberal democracies. In A. Barry, T. Osborne, N. Rose (Eds.). *Foucault and political reason: Liberalism, neo-liberalism, and rationalities of government*. (pp. 37-64). Chicago, IL: University of Chicago Press.

Schiller, H. (1995). The global information highway: Project for an ungovernable world. In J. Brook, & I. A. Bola (Eds.). *Resisting virtual life: The culture and politics of information*. (pp. 17-33). San Francisco: City Lights.

Schmidt, A. (2014). Open security, contributions of networked approaches to the challenge of democratic internet security governance. In R. Radu, J. Chenou, & R. H. Weber (Eds.). *The evolution of global internet governance: Principles and policies in the making*. (pp. 169-190). Berlin: Springer.

Seçen, T. (2006, June 12). Ekşi Sözlük ve diğer site kapatmaları üzerine-2. *Türk-internet.com*. Retrieved from: http://www.turk-internet.com

Spafford, E. H. (1989). The Internet worm: Crisis and aftermath. *Communications of the ACM*, 32(6). 678–87.

Şen, E. (2013, September 28). Şirketler internet sitelerine erişimi engelleyebilir mi?. *T24 Bağımsız İnternet Gazetesi*. Retrieved from: http://t24.com.tr

The Citizen Lab (2013) *Planet Blue Coat: Mapping global censorship and surveillance tools*. Toronto: University of Toronto.

Theodorelis-Rigas, H. (2013). From 'imagined' to 'virtual communities': Greek-Turkish encounters in cyberspace. *Studies in Ethnicity and Nationalism*. 13(1). 2–19

Topak, Ö. (2013). Governing Turkey's information society. *Current Sociology*. 61(5-6). 565-583.

Tuncer, A. M. & Yalçin, S. S. (1999). Multimedia and children in Turkey. *Turkish Journal of Pediatrics*. 41. 27-34.

Turkish Ministry of Transport, Maritime Affairs and Communications. (2013). National cyber security strategy and 2013 – 2014 action plan. Retrieved from: http://www.udhb.gov.tr/doc/siberg/ActionPlan2013-2014.pdf

Turkish Penal Law, Law Number 5651 (2007). *İnternet ortamında yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele edilmesi hakkındaki kanun*. Retrieved from: http://www.resmigazete.gov.tr/eskiler/2007/05/20070523-1.htm

Türk.internet.com. (2014, July 4). Aksünger : Erişim Sağlayıcılar Birliği nasıl kuruldu, kimler yer aldı, tüzüğü nasıl hazırlandı, neleri içeriyor?. *Türk.internet.com*. Retrieved from: http://www.turk-internet.com/

Usun, S. (2003). Educational uses of Internet in the world and Turkey (A comparative review). *The Turkish Online Journal of Distance Education*. 4(3).

Üstündağ, E. (2007, November 2). İnternet kafelere yaş sınırı getirildi. *Bağımsız İletişim Ağı (Bianet)*. Retrieved from: http://www.bianet.org

Winner, L. (1978). *Autonomous technology: Technics-out-of-control as a theme in political thought*. Cambridge, MA: MIT Press

Winner, L. (1993). Social constructivism: Opening the black box and finding it empty. *Science as Culture*. 3(3,16). 427–452.

Wolcott, P. & Çağıltay, K. (2001). Telecommunications, liberalization, and the growth of the Internet in Turkey. *The Information Society: An International Journal*. 17(2). 133-141.