SECURITIZATION OF CYBERSPACE GOVERNANCE AND THE RIGHT TO PRIVACY: CASES OF THE US, CHINA, AND ICELAND

A Master's Thesis

by

DURUKAN GÜVEN

Department of

Political Science and Public Administration

İhsan Doğramacı Bilkent University

Ankara

September 2021

To my family

SECURITIZATION OF CYBERSPACE GOVERNANCE AND THE RIGHT TO PRIVACY: CASES OF THE US, CHINA, AND ICELAND

The Graduate School of Economics and Social Sciences
of
İhsan Doğramacı Bilkent University

by

Durukan Güven

In Partial Fulfillment of the Requirements for the Degree of
MASTER OF ARTS IN POLITICAL SCIENCE

DEPARTMENT OF
POLITICAL SCIENCE AND PUBLIC ADMINISTRATION
İHSAN DOĞRAMACI BILKENT UNIVERSITY
ANKARA

SEPTEMBER 2021

I certify that I have read this thesis and have found that it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Arts in Political Science and Public Administration.

Prof. Dr. Pınar Bilgin
Supervisor

I certify that I have read this thesis and have found that it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Arts in Political Science and Public Administration.

Asst. Prof. Dr. Meral Uğur Çınar
Examining Committee Member

I certify that I have read this thesis and have found that it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Arts in Political Science and Public Administration.

Asst. Prof. Dr. Zerrin Torun
Examining Committee Member

Approval of the Graduate School of Economics and Social Sciences

Prof. Dr. Refet Gürkaynak
Director

ABSTRACT

SECURITIZATION OF CYBERSPACE GOVERNANCE AND THE RIGHT TO PRIVACY: CASES OF THE US, CHINA, AND ICELAND

Güven, Durukan

M.A., Department of Political Science and Public Administration

Supervisor: Prof. Dr. Pınar Bilgin

September 2021

This thesis adopts securitization theory to analyse the securitization of cyberspace governance in different parts of the world to understand how the securitization of cyberspace governance affects the right to privacy, because securitization and the right to privacy are intertwined. Every step taken by states regarding securitization has crucial impacts on the right to privacy either positive or negative manner. The thesis asks: "How do the USA, China, and Iceland securitize cyberspace governance, and what is the relationship between the securitization of cyberspace governance and the right to privacy in these countries?" To answer this question, the thesis analyzes the National Cybersecurity Strategies and Freedom on the Net reports that were published in the post-2015 period. The thesis observes a complicated relationship between the securitization of cyberspace governance and the right to privacy. What governments declare and the results of their actions in the securitization process can be inconsistent as in the US, can be consistent as in Iceland, and can be consistent and inconsistent at the same time as in China. According to the comparison of cases with each other, a free and not-free state can take non-democratic measures to secure cyberspace governance.

Key words: Securitization Theory, Cyberspace Governance, The Right to Privacy

ÖZET

SİBER ALAN YÖNETİŞİMİNİN GÜVENLİKLEŞTİRİLMESİ VE GİZLİLİK HAKKI: ABD, ÇİN VE İZLANDA ÖRNEĞİ

Güven, Durukan

Yüksek Lisans, Siyaset Bilimi ve Kamu Yönetimi

Danışman: Prof. Dr. Pınar Bilgin

Eylül 2021

Bu tez güvenlikleştirme teorisinden faydalanarak dünyanın farklı bölgelerindeki siber alan yönetişimlerini analiz etmektedir. Analizin amacı, siber alan yönetişiminin gizlilik hakkını nasıl etkilediğini anlamaktır çünkü güvenlikleştirme ve gizlilik hakkı iç içe geçmiştir. Güvenlikleştirme ile alakalı olarak devletler tarafından atılan her bir adım gizlilik hakkı üzerinde olumlu veya olumsuz yönde etki oluşturmaktadır. Tez "ABD, Çin ve İzlanda siber alan yönetişimini nasıl güvenlikleştiriyor ve bu ülkelerde siber alan yönetişiminin güvenlikleştirilmesi ile mahremiyet hakkı arasındaki ilişki nedir?" sorusunu soruyor. Tez bu soruyu cevaplamak için 2015 yılı sonrasında yayınlanmış olan Ulusal Siber Güvenlik Stratejilerini ve Freedom on the Net raporlarını analiz etmektedir. Tez, siber alan yönetişiminin güvenlikleştirilmesi ile mahremiyet hakkı arasında karmaşık bir ilişki gözlemliyor. Güvenlikleştirme sürecinde hükümetlerin beyan ettikleri ve eylemlerinin sonuçları ABD'deki gibi tutarsız, İzlanda'daki gibi tutarlı ve Çin'deki gibi hem tutarlı hem de tutarsız olabilir. Vakalar birbirleriyle karşılaştırıldığında, demokratik olan ve demokratik olmayan iki ülkenin, siber alan yönetişimini güvence altına alırken birbiriyle benzer şekilde demokratik olmayan önlemler aldığı gözlemlenmiştir.

Anahtar Kelimeler: Güvenlikleştirme Teorisi, Siber Alan Yönetişimi, Gizlilik Hakkı

ACKNOWLEDGMENTS

First of all, I would like to thank with most sincere to Prof. Dr. Pınar Bilgin. I will always remember her when I think about what a good teacher should be like throughout my life. The lessons I have learned from her, the way she teaches, and the way of thinking she conveys to the students in the lessons will contribute to me throughout my life. I am immensely grateful to Prof. Dr. Pınar Bilgin for being a very constructive and instructive thesis advisor. In addition, I express my appreciation to Dr. Meral Uğur Çınar for her support, who teaches courses that highly encouraged me to apply for graduate studies. The course that I took from her in my fourth year of BA studies was the trigger that finalized my decision for applying to the MA study. I will always be greatfull to her for helping me to choose my path.

I would also like to express gratitude to my mother, father, my lovely brother Efekan Güven. As a small note, Efekan is the best brother that I can ever imagine. As another member of my family, I am also very grateful to my love Elif Berka Tanyeli. She was with me in every process and in every struggle that I had faced in my MA adventure.

I owe special thanks to Elif Cemre Solmaz for listening to all my complaints regarding MA studies in hours of telephone calls. I would also be very grateful to Koray Berker Resber for all of his contributions to my thesis, being a perfect friend and future housemate. I am thankful to my companion Ceyhun Murathan Ünlü for being sided with

me for any condition. I would like to thank my VIP team who are Hanzade Tepeoğlu, Doğukan Kaya, Beyza Özgöde, Mehmet Günçavdı, and Eren Bilaloğlu.

I owe to special thanks for all their support to Burak Tatar, Özgür Uluçay, Artuğ Keremhan Bilgin, and Kürşad Doğan who have been with me since the first period of my Bilkent life.

And lastly, I also would like to thank myself for embarking on this adventure with determination and being able to finish my thesis with my patience and hard work.

TABLE OF CONTENTS

LIST OF TABLES

CHAPTER I

INTRODUCTION

Every state has its own method of securing the cyberspace. This thesis adopts securitization theory to analyse the securitization of cyberspace governance in different parts of the world. Securitization is an instrument that is used by political actors (Waever, 1995). Securitizing actor defines a certain issue as a security threat to a referent object via speech act and the aim is to gain control over the issue (Buzan et al., 1998). Definitions, referent objects, and methods to secure cyberspace differ among states and securitization theory can help to analyze these differences.

Cyberspace is an appropriate field to develop and examine new securitizing moves because states, societies, businesses individuals increasingly penetrate into cyberspace and the increasing penetration brings new threats and risks (Balzacq et al., 2016, p. 515). Political actors especially governments benefit from securitization as a tool against threats and risks in cyberspace so political actors can take exceptional measures for the provision of security.

Most states assume responsibility to create secure cyberspace as protection from malicious actors such as other states and hackers. However, the other critical point is a state's potential for becoming a malicious actor itself in cyberspace. A state can become

a security threat to the right privacy of its own citizens. States' methods to create more secure cyberspace also shapes their approaches to personal data (Deibert, 2002). An examination of securitization of cyberspace governance opens the way for analyzing the impact on the right to privacy.

This thesis has been written to understand how securitization of cyberspace governance affects the right to privacy, because securitization and the right to privacy are intertwined. Every step taken by states regarding securitization has crucial impacts on the right to privacy either positive or negative manner. This means that if we understand how cyberspace governance is securitized, we can understand to what extent our right to privacy is taken away or protected.

Research Question

To further understanding of the relationship between the right to privacy and securitization of cyberspace governance, the thesis asks the following research question: "How do the USA, China, and Iceland securitize cyberspace governance, and what is the relationship between the securitization of cyberspace governance and the right to privacy in these countries?" To answer this question, the thesis analyzes the National Cybersecurity Strategies and Freedom on the Net reports that were published in the post-2015 period.

This research looks for answers to the following 4 sub-questions in data for the comparison of cases. These questions are derived from the securitization theory (Buzan et al., 1998; Waever, 1995).

- What is the definition of security?

- What/Who are threats to security?
- What/Who is being secured?
- How is security addressed?

Answers to these questions can clarify the relationship between the right to privacy and the securitization of cyberspace governance.

According to Waever (1995) and Buzan, Waever, Wilde (1998), securitization theory can be summarized as below. Securitization starts with a speech act. A securitizing actor especially states and state elite uses speech acts to securitize an issue. The aim of securitization of an issue is to take control over it and to consider an issue beyond normal politics. So an issue moves from a normal level to a more prioritized level. A prioritized issue beyond can require exceptional measures that cannot be taken in normal politics. Referent objects can be protected from threats with these exceptional measures. The securitizing actor uses speech act to convince the audience on why there is a need for exceptional measures to secure a referent object. The audience can be actors inside or outside of a state or both of them.

Methodological Framework

This thesis applies a case study approach to explain and analyze the selected cases. The case study approach is useful to make deep analyses of selected cases. The thesis employs the most-similar method to analyze the cases of Iceland and the USA and it also employs the most-different method to analyze cases of China and the USA. This method allows us to study how some similarities among cases such as regime type can cause

different outcomes and some differences among cases can lead to similar outcomes. The outcome is the impact on the right to privacy.

This methodological design is beneficial to understand different schemas in the securitization of cyberspace governance and to see what kind of analysis can be made with these schemas. As stated, this thesis aims to analyze selected cases according to the answers to the 4 sub-questions mentioned above. The answers given to these 4 questions show how cases schematize the securitization of cyberspace governance. Here, schemas provide gathering cases in a common format so that the answers to similar questions can be compared and analyzed. A common framework is necessary to compare and analyze cases because data was created by different actors at different times.

A case study is a research approach that is based on an in-depth study of a single or a few instances (Blatter, 2008, p. 68). Single or a few cases are representative of a small number of samples. Gerring (2007) states that the method has to be qualitative and small-N, there has to be a specific type of research material, and the researcher has to analyze multiple sources of evidence. Both of the scholars highlight the necessity of a small-N sample size and Gerring (2007) adds that research material has to be certain and it should be created by various sources. Gerring provides some details about the data in case study. According to Gerring, "Evidence for a case study may be drawn from an existing dataset or set of texts or maybe the product of original research by the investigator. Written sources may be primary or secondary" (Gerring, 2007, p. 68).

The scope of causal inference is broad in the large-N cross-case study and deep in single/few case-study. This basically means that single/few case study is knowing more about the less but cross-case study is knowing less about more (Gerring, 2007, p. 49).

Knowing less about a large number of cases and knowing more about a single case is a matter of preference for the researcher. The decision is made according to the research design, goal of the research, and the research question.

Lijphart (1975) states distinctions among case study and cross-case study: The Large-N sample does not contain all the necessary research material about a single case. A large sample with too detailed/intensive data about every single case means a huge amount of data and that amount of data cannot be handled properly in social research (Lijphart, 1975). On the other hand, a case or a limited number of cases in small-N research designs can contain intensive/detailed information about every single case. Case or cases are selected logically for representativeness so the researcher can obtain a more representative outcome. It means that a non-randomly selected case does not have to be limited to its own in terms of insight, it can represent a wider universe.

However, Mahoney and Goertz (2006, p. 237) state that

> …in quantitative research, scholars usually define their scope more broadly and seek to make generalizations about large numbers of cases. Quantitative scholars often view the cases they analyze simply as a sample of a potentially much larger universe.

In other words, when the scope of research increases, the scope can refer to sample size, large-N cross-case analysis can reach more generalizable outcomes because the range of cases is not limited as in small-N studies. This does not mean that single/few case studies are limited to cases they explain because single/few case studies can represent a broad universe. Hancke (2009, p. 61) indicates that "…the case(s) is (are) representative of a wider set of instances in which something similar might happen".

According to Gerring (2007, p. 43), "Cross-case research is always more representative of the population of interest than case study research…". The reason is sample-size.

When the number of cases is grown, researchers can achieve more representative and generalizable outcomes. However, this does not mean that case study research analyses fewer data than cross-case study research. King, Keohane, and Verba (1994) highlight that case study researchers can work on a huge amounts of data sourced by a single case. In view of Gerring and Cojocaru, "A case study, for present purposes, is an intensive study of a single case or a small number of cases that promises to shed light on a larger population of cases" (Gerring & Cojocaru, 2016, p. 394).

How many cases a researcher studies on or how many observations the researcher's samples involve matter when research is decided. Gerring (2007) summarizes nine common case study types for the demonstration of various techniques for non-randomly case selection. Non-randomly means the selection of cases based on research goals. Those nine types are typical, diverse, extreme, deviant, influential, crucial, pathway, most-similar, and most-different. In the following part, the most-similar and most-different methods will be explained.

According to Gerring (2007) and Hancke (2009), the most-similar method contains at least a non-randomly selected two cases. Most-similar cases share some commonalities but differences are the dependent variable that is the outcome and the independent variable that explains the outcome (Gerring, 2007; Hancke, 2009). The most-different method contains at least non-randomly selected two cases that are different in every related observation. But cases are similar in both dependent and independent variables (Gerring, 2007; Hancke, 2009).

Most-similar and most-different method focus on certain observations that affect the outcome (Anckar, 2008, p. 400). In other words, "…a systematic matching and

contrasting of cases can be attempted that enables us to identify some key distinguishing or common variables while controlling for the others" (De Meur & Berg-Schlosser, 1996, p. 426). Skocpol's (1979) book *State and Social Revolutions: A Comparative Analysis of France, Russia, and China* and Yashar's (2005) book *Contesting Citizenship in Latin America: The Rise of Indigenous Movements and the Postliberal Challenge* employ both of the method of agreement and the method of difference at the same time. Certain observations, their impacts on the outcome, and systematic matching and contrasting of cases are observable in Skocpol (1979) and Yashar (2005)

Yashar (2005) uses the most-different method to make a cross-national comparison of Ecuador, Bolivia, Guatemala, and Mexico. The author states that indigenous movements emerged in all of these four cases despite their differences. Emergence of an indigenous movement is the outcome. However, the author also compare these four cases with Peru by using the most-similar method. Yashar says that "...Peru shares certain central features with several of the cases and yet failed to witness the emergence of a significant indigenous movement…" (Yashar, 2005, p. 23). Yashar (2005) summarizes certain central features: Peru, Ecuador, and Bolivia share basic geography, demography, and histories of populism and corporatism, additively, Peru and Guatemala had faced a violent civil war. Cases are similar in certain features mentioned above but the outcome is not similar when Peru and the other cases are compared.

Skocpol (1979, p. 37) says that France, Russia, and China are three cases of successful social revolution. Despite their certain differences, they share similar causal patterns. Skocpol (1979) selects England, Japan, and Germany as cases that did not experience social revolution in the past. Cases that did not experience social revolution demonstrate

some similar features with France, Russia, and China but the political crisis did not end up with a social revolution in England, Japan, and Germany. There are two groups of cases, the first group has faced with social revolution but the other one did not face a social revolution. It means that two groups of cases do not share the same outcome despite the similarities they share.

These two studies apply the combination of most-similar and most-different case selection method and they shows that some similar characteristics or observations of cases do not correctly explain outcomes all the time. These studies also confirm that some different characteristics or observations can lead to similar outcomes. A combination of most-similar and most-different method designs proves that differences among cases do not cause an obstacle to clarifying similar causal patterns and the similarities among cases may not be sufficient to explain the exact causal patterns (Skocpol, 1979, p. 38).

Three cases were non-randomly selected to apply the methodology. The first case is the US. The US (United States of America) is a country located in North America with around 330 million population. The number of internet users is around 297 million in 2020 and the Internet penetration rate is around 90 percent (*Internet World Stats*, 2021). Freedom house defines the US as a "free" democratic state because The US has a strong rule of law tradition and civil liberties and political rights are well respected in the US (*United States: Freedom in the World 2021 Country Report*, 2021). The US is another unique example to analyze the securitization of cyberspace governance. As a “free” and democratic state, security agencies widely use surveillance technologies to collect personal data which is a threat to the right to privacy.

China is a country located in East Asia with a 1.4 billion population. It is the most populated country in the world. The number of internet users is around 990 million in 2020 (*Internet World Stats*, 2021). The Internet penetration rate is around 68 percent. Freedom house defines China as a "not free" authoritarian state with more repressive tendencies in recent years (*China: Freedom in the World 2021 Country Report*, 2021). According to Freedom House, China is “the world’s worst abuser of internet freedom”. The ruling CCP (Chinese Communist Party) increases its authority upon other actors in China such as the media, universities, and internet users year by year. Political rights and civil liberties are under threat in China (*China: Freedom in the World 2021 Country Report*, 2021). China provides a unique example to analyze the securitization of cyberspace governance as the “worst abuser of the internet”.

Iceland is a country located in North Atlantic Ocean with around 340 thousand population. The number of internet users is around 337 thousand in 2020 and the Internet penetration rate is around 99 percent (*Internet World Stats*, 2021). Freedom house defines Iceland as a "free" parliamentary democracy and Civil rights and liberties are strongly protected in Iceland (*Iceland: Freedom in the World 2021 Country Report*, 2021). Iceland is another unique example to analyze securitization of cyberspace governance. According to Freedom House, Iceland is “the world’s best protector of internet freedom”.

There are two kinds of data used in this thesis related to each case. Data 1 is official cybersecurity strategy papers published by governments of the selected countries and it is an inside explanation to the securitization of cyberspace governance by selected states. Cybersecurity strategies are political acts and they create a discourse on cybersecurity

and awake an awareness among state, non-state, or private actors about the possible threats in cyberspace (Shackelford, 2016, p. 454). These strategy papers declare to the public that how states do securitize cyberspace governance, their aims to securitize, and why there is a need to secure cyberspace governance. The public comprises both the international community and their own citizens.

National Cyber Strategy of the United States of America was published by Trump's administration in September 2018 (*National Cyber Strategy of the United States of America*, 2018). China's *National Cyberspace Security Strategy* was published in December 2016 by the National Internet Information Office in both Chinese and English (*National Cyberspace Security Strategy - China*, 2016). *Icelandic National Cyber Security Strategy 2015-2026: Plan of action 2015-2018* was published by the Ministry of the Interior in June 2015 and the approved English version was issued too in April 2015 (*Icelandic National Cyber Security Strategy 2015-2026 Plan of Action 2015-2018*, 2015). These strategy papers are publicly available on the official web sites of related government institutions and these documents are the most recent published national cybersecurity strategy papers of these three countries.

Data 2 is 'Freedom on the Net' reports of selected country cases that are published by the Freedom House. "Freedom House produces research and reports on a number of core thematic issues related to democracy, political rights and civil liberties" (*About Us | Freedom House*, n.d.).These reports are published annually and publicly available on the internet.

Freedom on the Net provides an outside explanation of how states securitize cyberspace governance. These reports provide an examination of states by an independent

organization as objectively. They gather various sources related to the securitization of cyberspace governance. These sources can include news, laws, reports published by different think tanks, expert opinions, and individual experiences.

Data 1 and Data 2 answers 4 sub-questions from their own perspective and the goal is analyzing and comparing these differences. For each state, there are two schemas for the securitization of cyberspace governance. The first schema is the reflection of cybersecurity strategy papers and the second schema is the reflection of Freedom on the Net reports. The aim of creating two schemas is to show the differences between what states declare and what results of their actions are.

In the thesis, the time period is chosen based on the latest national cybersecurity strategy paper. The thesis covers the latest national cybersecurity strategy papers published in each case. It also covers Freedom on the Net reports that are published after the publishment of the latest national cybersecurity strategy for each country. For China, the strategy paper in 2016 and Freedom on the Net reports published in 2017, 2018, and 2019 are included. For the USA, the strategy paper in 2018 and the 2019 report are included. For Iceland, the strategy paper in 2015 and reports published in 2016, 2017, 2018, and 2019 are included. This thesis covers the years of 2016, 2017, 2018, and 2019.

The reason for this selection is to observe the impacts of cybersecurity strategy papers and compare what is discussed in strategy papers and what is happened after the publishment of strategy papers. Strategy papers are useful to understand securitization process and the effects on process can be examined via Freedom on the Net reports. Therefore, annual Freedom on the Net reports after publications of strategy paper are included in this thesis.

The rest of the thesis is divided into three chapters. The next chapter is the literature review. It reviews the literature on the securitization of cyberspace governance and its relationship with the right to privacy. The chapter separately reviews the governance of cyberspace, securitization theory, securitization of cyberspace governance, and studies of the securitization of cyberspace governance and its implications on the right to privacy. The third chapter presents the US, China, and Iceland cases based on data sourced by the national cybersecurity strategy papers and freedom on the net reports. This chapter is structured upon four main questions identified in the research question part. The final chapter is the conclusion. This chapter includes the analysis and conclusion of the thesis. It presents the main findings.

CHAPTER II

LITERATURE REVIEW

This chapter aims to review the literature on the securitization of cyberspace governance and its implications for right to privacy. For this purpose, the literature about cyberspace governance, securitization theory, and the securitization of cyberspace governance will be looked at. The first section reviews the cyberspace governance. The second section highlights securitization theory and some other approaches. The third section looks What is the securitization of cyberspace governance and what are reasons behind securitization? The fourth section reviews studies on the securitization of cyberspace governance and its implications on the right to privacy.

2.1. Governance of Cyberspace

Cyberspace is a virtual space separate from the physical world. Cyberspace is defined by the Oxford English Dictionary as: "The space of virtual reality; the notional environment within which electronic communication (esp. via the internet) occurs" (*Cyberspace*, n.d.). According to Kuehl (2009, p. 27), technological infrastructure should also be involved in the definition of cyberspace:

> Cyberspace is a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via

> interdependent and interconnected networks using information-communication technologies.

These two definitions of cyberspace focus on virtual space and physical infrastructure while leaving out human element.

Some other authors insist that human interaction is the other core component of cyberspace (Barlow, 1996; Fang, 2018; Loader, 1997; Rheingold, 1994; Whittaker, 2004). Rheingold (1994, p. 5) defines cyberspace as the conceptual space with various components that mediated by communication technology including words, people communication, data, wealth, and power. According to Barlow (1996), cyberspace is a new social environment, it is a place for freedom of expression where people can act without the fear of authoritarian power. Loader (1997, p. 1) offers a comprehensive definition for cyberspace:

> Cyberspace is a computer-generated public domain that has no territorial boundaries or physical attributes and is in perpetual use. To date its most potent manifestation is that matrix of electronic telecommunication and computer networks, usually referred to as the Internet, which links millions of people globally, is growing at a rapid rate daily, is taking new shape and direction as a consequence of the voluntary actions of its participants, and, it is claimed, is not controlled by any single authority.

Barlow (1996) and Loader (1997) include power relations in this new environment and they state that one power holder cannot control the whole cyberspace. The reason is that cyberspace can connect billions of people all around the world instantly, it is changing rapidly because of technological developments, and it is an endless space which has no boundaries. In parallel with Barlow and Loader, Fang (2018, p. 13) underlines that state and non-state actors can intervene in cyberspace for various purposes such as political, economic, security and scientific but it is not possible for the governance of cyberspace by a single entity. Therefore, cyberspace has implications on the attitudes of state,

society, and private actors and those attitudes can involve political, economic, cultural, and societal (Whittaker, 2004, p. 11).

Cyberspace is defined as a part of both physical and virtual space. These interdependent spaces connect billions of humans globally so the human factor is also involved. All of these three components (physical, virtual, and human) are a combination of their own. For example, computers are part of the physical sphere, the Internet is a part of the virtual sphere, and social media users are part of human involvement in cyberspace.

Working Group of Internet Governance (2005, p. 5) defines governance of cyberspace. According to WGIG's (2005) report, governments, private sector, and civil society are involved in the governance process and they are responsible for the development of shared principles, norms, and decision-making procedures. The goal of actors is modeling the transformation and the use of the internet. The working definition indicates that each stakeholder has various interests and roles.

According to Denardis (2014, p. 11), governmental, non-governmental, and private actors can regulate or govern the cyberspace. Governance of cyberspace does not involve a central government (Y. Shen, 2016, p. 83). In other words, interdependent factors are responsible to coordinate and regulate cyberspace as a part of the governance process and none of these actors are the only authority.

Beyond a central authority, there are several actors that involves governance of cyberspace, they are individual governments, international organizations, the private sector, non-governmental organizations, academics, and experts have to be a part of cyberspace governance (Mathiason, 2009, p. 23). Deibert and Rohozinski (2010a) also

underlines other actors such as civil society, criminals, millions of internet users, individual hackers.

Mathiason et al. (2004) describe three governance functions in cyberspace. The first function is technical standardization. Technical standardization considers the decisions about networking protocols, software applications, and data format standards. The second one is resource allocation and alignment. This function regards some scarce or exclusive elements of the Internet. The distribution of elements to users has to be coordinated. Those elements can be domain names and IP addresses. The third one is policy formulation and enforcement. "This function refers only to people and organizations directly involved in the design, operation, or use of the services and networks employing the Internet protocols" (Mathiason, 2009, p. 18). The first two functions are mostly governed by non-state actors and the third one mostly governed by state actors.

When the diversity of actors and functions are considered, there is not a single type of governance of cyberspace. Mueller (2010, p. 9) states that governance of cyberspace types is related to how cyberspace is coordinated, managed, and shaped to reflect policies. In other words, the governance of cyberspace is shaped by the main authority in governance, methods to govern cyberspace, and the main principle of governance.

Kobrin (2001, p. 688) has argued that cyberspace governance requires international cooperation and effective governance to keep the balance between the public and private sectors. Governance is not a domestic issue and public institutions are not the central authority in cyberspace. Actors outside of the borders of nation-states and private companies have to be involved cyberspace governance process. The reason is that

cyberspace does not have geographic borders and so what happens in the virtual world can create drastic effects on inside and outside borders (Kobrin, 2001, p. 690). Therefore, cyberspace goes beyond the borders defined by the national and international actors so private actors are also irreplaceable part of cyberspace governance.

As a parallel to Kobrin (2001), the multistakeholder governance model provides a formulation for cyberspace governance. This model includes adding more actors by governance such as private industry, international governance institutions, governments, technical community, and civil society (Jayawardane et al., 2015, p. 5). The multistakeholder approach relies on national and international level coordination by a group of actors for the implementation of internationally accepted norms and policies. In this manner, Denardis (2014, p. 23) proposes five methods to govern cyberspace: technical design decisions, private corporate policies, global institutions, national laws and policies, and international treaties.

However, Bauer (2005, p. 7) states that a general set of values and norms to regulate the global cyberspace cannot exist because every state has its dynamics that are based on regime type, culture, and societal norms. Cyberspace governance policies have to be specific enough to respond to the needs and interests of states but international actors cannot afford alone all national needs.

Moreover, some scholars focus on the potential risks in cyberspace governance related to democratic concerns. International cooperation and public-private balance do not achieve the common democratic norms to govern cyberspace. Hence, some states especially authoritarian ones, have adopted a state-centric approach to control

cyberspace. In these states, the multistakeholder approach in the governance process is not a concern or principle at this point.

Cyberspace consists threats to states especially authoritarian ones (Deibert & Rohozinski, 2010a; Mueller, 2010; Rød & Weidmann, 2015; F. Shen & Liang, 2015; Tucker et al., 2017). Cyberspace consist features that foster mobilization of opposition and protest against authority (Deibert & Rohozinski, 2010c). For example, communication technologies in cyberspace can become a tool for freedom as opposed to an authoritarian power, since it is hard to control and information flow is too fast in cyberspace (Rød & Weidmann, 2015). There is a scholarly agreement that components of cyberspace (especially the Internet) put pressure on states (especially authoritarian ones). This is because it globalizes the scope of communication, it increases the scale of communication, it distributes control, and it leads to grew new institutions (Mueller, 2010, pp. 4–5).

However, there are authoritarian methods to govern cyberspace as oppose challenges that are mentioned above. As opposed to approaches that include multiple actors in governance of cyberspace, some states want to be the only power in domestic cyberspace and even outside of their domestic sphere. Hence, this kind of approach does not accept international cooperation and involvement of various actors in the governance process. The involvement of other actor can lead to separation of power and rising opposing opinions. The desire to be the only sovereign power inside or outside of domestic cyberspace creates a way forward to authoritarian cyberspace governance. For example, the main aim of China in cyberspace governance is the protection of state sovereignty to make independent cyber policies (Y. Shen, 2016). Chinese government

follows authoritarian cyberspace policies to be a single authority in governance for the protection of state sovereignty.

In addition, authoritarian management of cyberspace can take advantage of filtering technologies, internet censorship, and surveillance (Deibert & Rohozinski, 2010a). Easy communication and rapid information sharing can also lead to undemocratic consequences because state elites can gain more control over information flow for their purposes via the internet (Entman & Usher, 2018). Furthermore, autocrats can aim to limit online opposition via fear tactics, they can promote government propaganda via online bots, and finally, they can spread illiberal values on cyberspace especially on social media (Tucker et al., 2017). Cyberspace governance can lead to undemocratic results in authoritarian states as opposed to democratic governance models.

There are three core components in cyberspace; physical, virtual, and human (Rheingold, 1994). The combination of three components creates cyberspace and it changes the way for human interaction especially via social media. The new way of social communication provide a space for the freedom of opinion (Barlow, 1996). But cyberspace can become a repression tool against to freedom of opinion and right to privacy (Deibert & Rohozinski, 2010b). States, governments, private sector, civil society, experts, individual hackers, academics, smart devices, intelligence agencies, and the Internet users are some of the examples of the actors in cyberspace and all of them are involved in the governance process. Being only one central governance actor in cyberspace is not possible (Fang, 2018; Y. Shen, 2016)

2.2. Securitization Theory

Securitization theory was developed by the Copenhagen School. Weaver's (1995) article "Securitization and Desecuritization" and Barry Buzan, Ole Waever, and Jaap de Wilde's (1998) co-authored book *Security: A New Framework for Analysis* are texts in securitization literature. This section presents an overview of securitization theory. Securitization theory is helpful to think about governance of cyberspace because various actors especially some states securitize cyberspace governance. How actors securitize cyberspace governance is different case by case and these differences can be examined with the help of securitization theory. In this thesis, my aim is to analyze how states securitize cyberspace governance by utilizing securitization theory. The first part looks at what is securitization theory and the next section reviews other perspectives on the theory.

Waever (1995) asks: "What really makes something a security problem?" He states that something is defined as a security problem by some actors and these actors are usually states and their elites. The securitizing actor uses speech act to raise a specific issue to a prioritized level. A securitizing actor would transform an issue into a security problem by the use of language and this is how security is regarded as a speech act (Waever, 1995). The goal of the declaration of some issues under security terms is to gain control over the issue. "A problem would become a security issue whenever so defined by the power holders" (Waever, 1995). Therefore, the speech act is a way for persuasion used by a securitizing actor and the actor uses language to convince the audience.

Copenhagen School states that "Security is the move that takes politics beyond the established rules of the game and frames the issue either as a special kind of politics or

as above politics" (Buzan et al., 1998, p. 3). Securitization of an issue requires exceptional measures or solutions beyond normal politics. "Securitization is a more extreme version of politicization" (Buzan et al., 1998, p. 23).

Measures in securitization process is a way to secure the referent object. Actors such as states and state elites make a move to securitize issues for the protection of referent objects. Securitizing actors are the ones who securitize issues because of potential threats to the referent object. The referent object can be defined as "things that are seen to be existentially threatened and that have a legitimate claim to survival" (Buzan et al., 1998, p. 36). In this manner, Buzan et al. (1998, p. 5) say that:

> Threats and vulnerabilities can arise in many different areas, military and nonmilitary, but to count as security issues they have to meet strictly defined criteria that distinguish them from the normal run of the merely political. They have to be staged as existential threats to a referent object by a securitizing actor who thereby generates endorsement of emergency measures beyond rules that would otherwise bind.

The securitizing actor has to convince the audience about the existential threat that poses harm to referent objects (Buzan et al., 1998, p. 25). Without the acceptance of the audience, securitizing actors cannot take extraordinary measures to secure referent object. In other words, the securitizing actor needs to convince the audience for framing an issue as a threat and so the actor can get acceptance to get extraordinary measures that cannot be taken in normal politics (Buzan et al., 1998, p. 26).

I will now look at some other approaches and contributions to securitization theory. Waever (1995) presents security at three levels, these are international level, national (state) level, and individual level. However, Waever (1995) analyses security at the national (state) level. In this, Waever (1995) pointed out that:

> We can then strip the classical discussion of its preoccupation with military matters by applying the same logic to other sectors, and we can de-link the discussion from the state by applying similar moves to society. With this, we maintain a mode of thinking, a set of rules and codes from the field of "security" as it has evolved and continues to evolve.

The method of security analysis at the state level can be both applicable to international or individual level. The method consists of a specific set of actions, rules, and codes. For each level, codes and rules can change but the logic will be the same.

Waever (1995) identifies international and individual levels of security but he does not describe all of them in detail. Securitization of cyberspace governance can be analyzed at global level since threats are not domestic. There is a need for international cooperation to cope with threats in cyberspace and some states such as Iceland defines cyber threats as a global problem in their strategy papers (*Icelandic National Cyber Security Strategy 2015-2026 Plan of Action 2015-2018*, 2015).

Buzan & Waever (2009) presents “macrosecuritization” in their article to further understanding of national level and international level dynamics. In the article, they underline six levels of analysis; Global level, System-level, Civilisational, Unit level, Group level, and Individual level. The global level comprises the whole planet and the unit level is mostly composed of states and nations. Buzan and Waever (2009) argues that the securitization theory focuses on middle-level (national level) securitizations and it does not explain macro (Global) or micro (individual) level securitizations in detail.

A successful macrosecuritization needs to fulfill the same criteria with the other securitizations but the main distinction is that it seeks to explore securitization on a larger scale (Buzan & Wæver, 2009, p. 257). Universal religions or political ideologies are two examples of larger scaled referent objects (Buzan & Wæver, 2009, p. 257). In

other words, a securitizing actor can securitize the environment as a referent object, against possible threats such as high rates of CO2 emission. Environment should not only be securitized by a single state, it is a global issue because it causes a threat to humankind on a planetary scale (Buzan & Wæver, 2009, p. 261). In other words, macrosecuritization needs to follow the same route (securitizing actor, speech acts, and responsive audience) with other securitizations to obtain success but its scale is much broader than mid-level securitizations based on their referent objects.

As another contribution offered by Aradau (2004), securitization theory does not cover the concept of desecuritization both politically and analytically in a detailed manner (p. 389). In this line, the Copenhagen School presents a dichotomy between normal politics and extraordinary politics since a successful securitization has to move issues from normal to extraordinary politics. The necessity of extraordinary measures to secure referent objects can be regarded as a threat to the democratic process when a specific example of securitization is analyzed (Aradau, 2004; Bigo, 2002; Neal, 2012; Williams, 2015). In this line, state actors usually securitize cyberspace and move issues from normal politics to extreme politics for different purposes. Even though the method to secure cyberspace violates the right to privacy, some of the authoritarian states such as China and Russia securitize cyberspace for getting extraordinary measures.

In a democratic state, the securitization can become a dangerous tool against democracy since it normalizes exceptional measures. Aradau (2004, p. 393) states that:

> In this context, desecuritization becomes an ethical-political choice which refuses to let democratic politics slip into exceptional politics. If the slowness of procedures ensures the possibility of contestation, the speed introduced by security does away with the possibility of scrutiny as well as the expression of voice.

Exceptional politics can provide speed to secure the reference object, but at the same time, it can cause undermining of different voices in democratic politics and can prevent checks upon exceptional measures by other actors. Aradau (2004) says that "The exceptional politics of securitization turns into a dangerous undertaking for democracy" (p. 393).

The author underlines that the securitization brings with extraordinary measures to move from normal politics to exceptional politics. The aim is to make rapid responses to the security threats and so the theory advocates speed against the slowness of the democratic process. In Aradau's (2004) view, "The speed required by the exceptional suspends the possibilities of judicial review or other modalities of public influence upon bureaucratic or executive decisions"(Aradau, 2004, p. 392). Politics of extraordinary is defined as making decisions as independent from the rules of normal politics (Williams, 2015, p. 115). Therefore, the securitizing actor legitimizes the exceptional policies in the eyes of the audience but these extraordinary measures can even be illegitimate in normal politics.

Security professionals such as officials and bureaucrats can exaggerate existent security threats or even they can securitize any other issue as a source of insecurity for their interests. On this issue, Bigo (2002, p. 61) stated that security professionals may manage insecurities as a way to follow their bureaucratic interests. The author analyzes various explanations concerning the securitization of migration to provide evidence to the above-mentioned argument. Immigration becomes a security issue when presented by security actors especially the state, government, or even society; this is a way of managing insecurities and also getting advantage of securitization for institutional or

individual interest (Bigo, 2002, p. 64). In the end, securitization is regarded as a tool to administer fears caused by insecurities and these insecurities are not inherent, they are the consequences of speech acts by actors. These actors can be benefited from this discursive power for their bureaucratic interests, the main purpose does not have to be the security of the referent object.

This thesis focuses on methods to secure cyberspace governance and some methods to secure cyberspace can lead to democratic threats. Aradau (2004) and Bigo (2002) underline these potential democratic threats and this thesis also aims to clarify threats to democracy caused by the securitization of cyberspace governance.

To summarize, securitization theory starts with a speech act to shift issues from normal to a prioritized level. A securitizing actor uses language to refer to a normal issue as a security matter. The aim of carrying issues to a prioritized level is to open the way for extraordinary measures. The securitizing actor takes exceptional measures to deal with security issues. Securitization also needs the approval of the audience before getting extraordinary measures. Taking extraordinary measures will be possible, only if the securitizing actor convinces the audience about the urgency and dangers of the issue that has to be securitized.

Buzan and Waever (2009), Aradau (2004), and Bigo (2002) present some contributions to the theory and different perspectives to securitization. Buzan and Waever (2009) indicate that Waever (1995) does not put sufficient attention to the analyses of individual or international level securitizations. Bigo (2002) says that securitizing actor especially governments securitize some issues to cover their own failures. From a different standpoint, Aradau (2004) emphasizes some threats to democratic governance which can

be led by exceptional measures led by securitization. More security can become a failure since normal politics is not able to deal with some issues without extraordinary measures (Buzan & Wæver, 2009, p. 29).

2.3. Securitization of Cyberspace Governance

Securitization theory has been applied in the study of cyberspace. This section provides an overview of the securitization of cyberspace governance literature. Key authors are Cavelty (2013), Cavelty & Egloff (2019), Deibert (2002), and Hansen & Nissenbaum (2009).

In cyberspace, referent objects can be government, business, and individuals. There are also malicious actors such as hackers, zealots or disgruntled insiders, criminals, terrorists or other malevolent groups, commercial organizations, and states (Hundley & Anderson, 1997, p. 232). According to Ramirez, "Risks in cyberspace are some of the main priorities of individuals, corporations, or governments because the wrong use of these critical infrastructures may lead to authentic threats to our economy, our productivity, and our security" (Ramirez, 2017, p. 142). In other words, threats in cyberspace can lead to insecurities at the macro, middle, or micro-levels.

Deibert (2002) presents four collective images about the securitization of cyberspace (especially the internet) governance. Images can be defined as different modes of securitization based on the variety in referent objects, securitizing actors and the method for providing security. Four collective images are stated as "national security", "state security", "private security", and "network security". Deibert (2002) points out that these images are ideal types and they can be different in practice. The assumption is that "States hold position and elites make a statement to fuse together elements of all four"

(Deibert, 2002, p. 118). Deibert (2002) does not claim that these four images are applicable for every practice of securitizations, they represent general schema of cyberspace securitization.

Deibert's (2002) first schema of securitization of cyberspace governance is the 'national security' image. "National security" image prioritizes the security of collective identities so the protection of nation and culture is the main concern. The Internet is seen as a threat to cultural security (Deibert, 2002). Referent objects are nation and culture. Securitizing actors are government and state. Complete isolation of the state, promotion of national values in cyberspace especially on the Internet and active state intervention to cyberspace are common ways to secure national identity (Deibert, 2002, p. 121). The second one is "state security" image. According to this image, the Internet can be used for strategic military purposes and it is a new medium of warfare (Deibert, 2002, p. 122). "State security" image prioritizes the security of physical infrastructure in cyberspace, state power, and authority over information flow. Referent objects are technological infrastructure, state power, and authority. For this purpose, the securitizing actor can build firewalls in cyberspace to restrict access and it can also distribute information flow to secure referent objects (Deibert, 2002, p. 125). The third on is 'private security' image. "Private security" image prioritizes the individual privacy. The referent object is the internet user and especially right to privacy. For this purpose, strict privacy regulations/rules that protect personal data is the way to secure democratic values (Deibert, 2002, p. 128). The fourth one is "network security" image. "Network security" image prioritizes the security of network and ICT (Information and Communication Technology) infrastructures. Referent object is ICT infrastructure. Development and

distribution of highly sophisticated encryption technology, systems of secure access and digital immune systems are common ways to network and ICT infrastructures (Deibert, 2002).

As another key author in cyberspace securitization, Cavelty (2013) presents various schemas of the securitization of cyberspace. The schema includes four clusters based on main actors, referent objects, and threats. Cluster, modality, and images can be defined as the schema of cyberspace securitization but authors choose different terms to explain these schemas. According to the first cluster, securitizing actors are security experts and they aim to secure computers and computer networks, and threats are malware, network disruptions, and hackers (Dunn Cavelty, 2013, p. 109). For the second cluster, securitizing actors are business, anti-virus industry, law enforcement, and intelligence community. The security of the private sector (business networks) and classified information (government networks) are prioritized. In this manner, threat sources are advanced persistent threats (malware), cyber-criminals (non-state), and cyber-spies (state) (Dunn Cavelty, 2013, p. 109). The third cluster presents civil defense and homeland security as securitizing actors. Referent objects are critical (information) infrastructures and society. Disruptions in critical infrastructures, cyber-terrorists (Nonstate), and cyber-commands (State) are the sources of insecurities (Dunn Cavelty, 2013, p. 109). According to the fourth cluster, securitizing actors are the military which aims to protect the networked armed forces (military networks) and nation/state. In addition, threat sources are particular attacks on critical infrastructures, cyber-terrorists (nonstate), cyber-spies (state), and cyber-commands (state) (Dunn Cavelty, 2013, p. 109).

Hansen and Nissenbaoum (2009) schematize securitization of cyberspace governance from their own perspectives as different from Deibert's schemas. Hassen and Nissenbaum (2009) provide the term "modalities of securitization" to define different schemas of cyberspace securitizations. Under the modalities of securitization, "network" and "individuals" are two of the referent objects for the securitization of cyberspace, but they are linked to broader referent objects such as the state, society, the nation, and the economy (Hansen & Nissenbaum, 2009, p. 1155). Their schemas are "hypersecuritization", "everyday security practices", and "technifications".

Hypersecuritization focuses on the speed and interconnectivity aspects of cyberspace. According to Hassen and Nissenbaum (2009), cyberspace consists threats such as malicious software and these threats can cause fatal hazards on society, finance, and military. Disasters in cyberspace can create a sequence because objects that are targeted by malicious actors in the cyberspace are somehow interconnected to each other. Hypersecuritization moves beyond mere securitization since cyberspace includes fatal insecurities and these insecurities can cause irrecoverable destruction on referent objects (Hansen & Nissenbaum, 2009, p. 1164). According to Deibert and Rohozinski, "Cyberspace is the domain through which electronic clearances take place, irrigation systems are controlled, hospitals and educational systems interconnect, and governments and private industries of all types function" (Deibert & Rohozinski, 2010c, p. 18). In other words, hospitals and educational systems are the examples of referent objects in cyberspace and the protection of these objects require high-level precautions. According to Hansen & Nissenbaum (2009), cyber destruction of these components may cause irresolvable problems.

The second security modality presented by Hansen and Nissenbaum is "everyday security practice" and it focuses on the impact of threats in cyberspace for everyday life. The main concern is to include users of the Internet in the securitization of the cyberspace process (Lobato & Kenkel, 2015, p. 31). It means that the Internet users should secure cyberspace against the possible threats. However, the Internet users can generate insecurities as a result of their irresponsible behavior such as spreading virus-infected files on the net (Hansen & Nissenbaum, 2009, p. 1166). Hansen and Nissenbaum (2009) states that the main securitizing actor makes the Internet users also responsible for securitization and the aim is the reduction of threats especially posed by individuals such as hackers in cyberspace.

The third security modality is "technification". The goal is creating and expanding a technical and expert discourse (Hansen & Nissenbaum, 2009, p. 1166). "Technifications play a crucial role in legitimating cyber securitizations, on their own as well as in supporting hypersecuritizations and in speaking with authority to the public about the significance of its everyday practice" (Hansen & Nissenbaum, 2009, p. 1168). In line with Hansen and Nissenbaum (2009), the spread of technical and expert discourse influences the audience positively about cyber securitization and the decisions made by experts for security purposes gain legitimacy in the eyes of the audience.

Cavelty & Egloff (2019) analyze different roles of the states in cyberspace from theoretical, empirical, and normative dimensions. Empirical dimension identifies 6 roles of state in cyberspace: (1) security guarantor, (2) legislator and regulator, (3) supporter and representative of the whole of society, (4) security partner, (5) knowledge generator and distributor, and (6) threat actor (Dunn Cavelty & Egloff, 2019, p. 37). As different

from above mentioned different schemas for the securitization of cyberspace governance, Cavelty & Egloff (2019) provides detailed analyses for the states' role in cyberspace governance as one of the main securitizing actor.

According to the security guarantor role, the state is the legitimate protector of its own civil and military networks against all types of cyber threats caused by technical and other means (Dunn Cavelty & Egloff, 2019, p. 49). The second role is legislator and regulator which means that the state acts as the legislator in cyberspace to provide legal order to clarify its hierarchical function vis-à-vis society and the economy. In addition, the state balances the relationship between citizens and businesses via laws and regulations in cyberspace (Dunn Cavelty & Egloff, 2019, p. 49). Deibert and Rohozinski state that "States seek policy coordination and regulations so as to make cyberspace a more secure, safe, and predictable environment recognizing its strategic importance to economic and social development" (Deibert & Rohozinski, 2010c, p. 17). The third role of the state is defined as: "State institutions act as supporters/ representatives of society by advocating for international frameworks that are conducive to both the respective economy and civil society" (Dunn Cavelty & Egloff, 2019, p. 49). International legal order and frameworks are supported by the state to govern cyberspace. The security partner role is about the provision of security via public-private partnership since dealing with the threats in cyberspace requires cooperation among actors and this cooperation is usually happening in the field of information exchange (Dunn Cavelty & Egloff, 2019, p. 49). The state also acts as a knowledge generator and distributor. It means that the state becomes a reliable information source for citizens and it aims to raise awareness, among the public, about the threats in cyberspace (Dunn Cavelty & Egloff, 2019, p. 49).

Therefore, the state acts as a securitizing actor and creates a public discourse concerning the audience. The sixth role defined by Cavelty and Egloff (2019) is “threat actor”. In this role, the state becomes a threat source in cyberspace; it generates insecurities in cyberspace (Dunn Cavelty & Egloff, 2019, p. 50). To clarify, domestically, some state activities such as surveillance that is a potential threat to the right to privacy and also internationally, “…political and economic espionage emanating from foreign states reinforce the perception of states as sources of danger” (Dunn Cavelty & Egloff, 2019, p. 50).

Deibert (2002) and Cavelty (2019) provide several referent objects for different schemas of the securitization of cyberspace governance. On the other hand, Hansen and Nissenbaum (2009) states that, reference objects, especially networks and individuals, cannot be analyzed independently with each other as stated by Deibert (2002) and Cavelty (2013). Referent objects are linked with each other. So when analyzing different securitization of cyberspace governance, reference objects and securitization methods should be examined separately, and also related larger referent objects should be included in the analysis.

2.4. The Study of the Securitization of Cyberspace Governance and its Implications on Democracy

This part aims to review the studies on securitization of cyberspace governance and its implications on democracy. Key authors are Ad’ha Aljunied (2019), Deibert and Rohozinski (2010c), Deibert and Crete-Nishihata (2012), Deibert (2018), Eldem (2019), Gorr and Schüneman (2013), Howard (2018), Kingsmith (2013), and Opderbeck (2012).

One of the key studies by Deibert and Rohozinski (2010c) demonstrates two-sides of securing cyberspace. The one side of securing cyberspace underlines the fundamental motives for securitization. The other side underlines the possible undemocratic consequences of securing cyberspace. According to Deibert and Rohozinski (2010c), the main argument is that governments make policies to securitize cyberspace governance against threats in cyberspace and the reason for securitization is provision of a more secure place economically and socially. However, securitization of cyberspace can lead threats to democracy such as filtering, self-censorship through pervasive surveillance, and even disconnection or disabling of physical internet infrastructure (Deibert & Rohozinski, 2010c, p. 17).

Ad'ha Aljunied (2019) examines the securitization of cyberspace governance in Singapore. The article underscores two main aspects of the securitization of cyberspace governance in Singapore. The first aspect of cyberspace governance is protection of critical information infrastructure from cyber threats (Ad'ha Aljunied, 2019, p. 5). The second aspect is "Online content regulation is driven by concerns over maintaining regime legitimacy, social cohesion and resilience in a multi-racial and multi-cultural society with a history of racial tensions and riots" (Ad'ha Aljunied, 2019, p. 1). In other words, the first aspect prioritizes the security of virtual and physical infrastructure. As second aspect, cyberspace turns into a tool for strengthening state authority in dealing deal with domestic problems.

As an example of different schemas of cyberspace securitization, Gorr and Schüneman (2013) conduct an analysis of elite discourse which is about cybersecurity based on official and open access documents in the cases of Germany and Russia. The study aims

to demonstrate similarities and differences in the governance of cyberspace. The study finds that both of the countries have securitized cyberspace governance while Russia defines the stability of the political system as the referent object instead of the stability of the economy as in Germany (Gorr & Schünemann, 2013). The author concluded that Russia follows state-centric regulations against cyber threats but Germany pursues a mediating role in cyberspace and regards international cyber norms (Gorr & Schünemann, 2013).

Opderbeck (2012) analyses four major cybersecurity proposals in the US between the years 2009-2012 such as the Cybersecurity Acts of 2009-2010. Opderbeck (2012) classifies cybercrime, cyberwarfare, and cyberterrorism as three sources of threats in cyberspace. The article concludes that national governments and international policymakers are the main securitizing actors against these three threats in cyberspace (Opderbeck, 2012). But the provision of security against cyber threats can cause threats to civil liberties. Specifically, the main argument of the study is that executive power has to consider the balance between cybersecurity measures and civil liberties since the intervention of Internet access such as censorship in the name of security can become a potential tool that undermines democracy (Opderbeck, 2012).

Eldem (2019) concludes that Turkey pursues a multilateral approach to cyberspace governance because domestic governance is close to authoritarian in line with information controls and the goal of establishing national cyberspace. However, in the international arena, Turkey acts in line with a multi-stakeholder approach that prioritizes free, pluralist, and open cyberspace governance (Eldem, 2019). It means that cyberspace governance inside and outside of Turkey is in tension with each other. This shows that

one state can follow two different schemas for the securitization of cyberspace governance.

The above part shows various schemas for the securitization of cyberspace governance. Schemas consist of examples of democratic or non-democratic approaches to secure cyberspace governance. In this part, non-democratic approaches are examined in detail. Deibert and Rohozinski (2010a) define three generations of cyberspace control. First-generation control is simple prevention of access to Internet resources by blocking access to servers, domains, keywords, and IP addresses. The second one is about the creation of a legal and normative space that aims to legalize denying access to information by state actors. The third generation control of cyberspace is the complex one. Manipulation of information, disinformation campaigns against opponents to authority in a state, and surveillance are three examples of the third generation control of cyberspace (Deibert & Rohozinski, 2010a, p. 27).

Gunitsky (2015) categorized four mechanisms to show how cyberspace can be used for non-democratic purposes by autocratic regimes so cyberspace especially social media can become a potential tool of regime stability. Those mechanisms are counter mobilization, discourse framing, preference divergence, and elite coordination. The author specifically analyses cases of Russia, China, and the Middle East to describe how those mechanisms can affect electoral democracy and state-society relations. The comparative analyses conclude that:

> Namely, social media has enabled non-democratic incumbents to safely gather previously hidden or falsify information about public grievances, to increase the transparency of the performance of local officials, to bolster regime legitimacy by shaping public discourse, and to enhance the mobilization of their support base (Gunitsky, 2015, p. 42).

The author explains that cyberspace especially social media can easily be used for non-democratic purposes.

Deibert and Crete-Nishihata (2012, p. 339) ask that "How is power exercised in and through cyberspace?" and more specifically, "How nondemocratic states outside of Europe, North America, and parts of Asia have begun to forcefully assert their interests in cyberspace governance regimes?". This article argues that the state's policies in cyberspace are shaped in parallel with the other states' actions since some international and global dynamics promote the spread of cyberspace controls. For example, "General statements about the war on terror or copyright controls can be turned into excuses for a broad spectrum of otherwise nefarious actions by authoritarian regimes" (Deibert & Crete-Nishihata, 2012, p. 354). In more detail, as a negative international dynamic, state intervention to cyberspace is increasing in authoritarian states and so some other western democracies also become more active in cyberspace via strict control and regulation as non-democratic states do. The main argument is explained and supported via textual materials (Internet governance policies) and cases from states such as the SMS ban in India, China, and Egypt.

Howard (2018) underlines that democracy especially free and fair elections should be protected from cyber-attacks but cybersecurity measures can also create challenges to democracy. The author describes four ways of intervention to democratic elections by domestic and foreign governments; " (1) manipulating facts and opinions that inform how citizens to vote, (2) interfering with the act of voting (3) changing the vote results, and (4) undermining confidence in the integrity of the vote" (Howard, 2018, p. 1367).

Additionally, Howard (2018, p. 1367) states that “In the name of national security, many governments have increased their cybersecurity efforts, which often includes the monitoring of their own people”. Therefore, in Howard’s (2018) view, cybersecurity measures are a need to protect democracy from domestic and international interventions but these measures have to comport with democratic values such as right to privacy.

After the review of some non-democratic approaches in the securitization of cyberspace governance, as an alternative to state-centric or non-democratic modes of cyberspace governance, Deibert (2018) explains the reasons for the necessity of a human-centric approach to cybersecurity. In the meantime, most of the cybersecurity policies center the national-security approach and so the main principle is the protection of sovereign states (Deibert, 2018, p. 411). In this line, the article explores the answers to the question: What are the possible consequences of the national-security approach to cybersecurity and why does cybersecurity governance need to be centered on the human security approach? The next point explains the main argument, which indicates that the dominant national-security approach to cybersecurity can violate human rights. “In the face of such threats, the national security-centric approach to cybersecurity is holding sway, funneling resources, power, and authority to the least democratically accountable agencies” (Deibert, 2018, p. 421). Alternatively, there is a need for a human-centric approach since it prioritizes the security of human rights (such as freedom of opinion, freedom of getting information, and right to privacy) instead of prioritization of state sovereignty in the national-security approach.

In this regard, Brown et al. (2012) say that cyberspace governance to establish secure and stable cyberspace has to be compatible with human rights but in practice,

securitization of cyberspace governance does not put sufficient attention to human rights such as freedom of expression and they even undermine such rights. The author also adds that cyberspace governance without democratic concerns decreases transparency and leads to a lack of accountability (Brown et al., 2012).

The last part of the literature review analysis the studies on the securitization of cyberspace governance. When the scholarly literature in this part considered, the schema for the securitization of cyberspace governance changes according to regime type, securitizing actors, referent actors, and response to threats. According to studies written by Deibert (2002), Ad'ha Aljunied (2019), Kingsmith (2013), and Howard (2018), there are two sides to the securitization of cyberspace governance. The first side indicates that there are so many vulnerabilities in cyberspace and referent objects such as individuals and networks are under threat. The other side concerns methods to secure cyberspace because the securitization of cyberspace can create some other threats to civil rights and liberties. It means that the securitization of cyberspace governance can lead to threats to the right to privacy. Some states can use the securitization of cyberspace governance as an authoritarian tool against the right to privacy. The cases for Singapore, China, and Russia are examples of using securitization as an authoritarian tool and as a method for normalization of exceptional measures such as untargeted surveillance.

2.5. Conclusion

Chapter 2 reviewed the literature on securitization theory, cyberspace governance, and securitization of cyberspace governance. The purpose of the literature review is to explain the concepts used in the theme of the thesis and to examine the studies related to the research topic. In the first two parts, the securitization theory and cyberspace

governance are explained. The third part examines how cyberspace governance and securitization are brought together in the literature. This review provides us various schemas of the securitization of cyberspace governance in the literature. In the 4th part, articles related to the securitization of cyberspace governance and its implications on democratic rights especially the right to privacy were reviewed.

Cyberspace has a complex structure consisting of 3 main components as physical, virtual, and human. This structure, which has no definite boundaries, can change very quickly and brings together millions of different dots such as humans or computers at the same time. Various actors are involved in the governance of this complex structure. Examples of these actors include states, non-state actors, civil society, private companies, individuals, and hackers. Cyberspace, which has an unlimited area, is rapidly changing, contains too many actors, and harbors millions of threats and vulnerabilities. When these features are taken into consideration, cyberspace governance also becomes quite complex. Actors are aware of these threats and they securitize cyberspace governance to protect referent objects. So different schemas of the securitization of cyberspace governance are used by different actors and differences are based on threats, methods to secure, and referent objects.

This thesis focuses on how states securitize cyberspace governance in the cases of the USA, China, and Iceland. There are two sides to how states securitize cyberspace governance. First, states should securitize cyberspace because cyberspace contains too many threats such as malware and hackers. These threats can harm many things within the state, such as the government, political system, and citizens. However, while states secure cyberspace, they may also lead to the emergence of new threats, especially in

terms of democracy. For example, the surveillance of citizens due to national security reasons can violate the right to privacy.

CHAPTER III

CASE STUDIES

The aim of the chapter is to analyze cases by focusing on the following questions.

- What is the definition of security?
- What/Who are threats to security?
- What/Who is being secured?
- How is security addressed?

The purpose of asking questions is to understand how selected cases securitize cyberspace governance. The thesis makes within and cross-case comparisons based on the answers to the above questions.

National cybersecurity strategies are a guide for analyzing securitization of cyberspace governance in China, the USA, and Iceland. Cybersecurity strategies are not fixed or all of them do not follow the same structure, goals, and attributes. Every state reflects their own way of governance in cyberspace, even a single state can publish dissimilar strategies in various time series. Selected cybersecurity strategies only represent the time period that is discussed to cover in strategies.

The other research material I will use is called Freedom of the Net Report by Freedom House. This report provides a measurement method in order to determine whether the

countries are free, partly free, or not free in regards to their digital media and the extent of internet freedom. The index measures these concepts by considering the various actors such as governmental, non-governmental, and private organizations. The reason why such consideration was taken is related to influences over digital media freedom because for Freedom of the Net index the states are not solely actors that had influence over the internet freedom or digital media freedom. The methodology of the report classified questions to measure the concept under three categories. The first category "Obstacles to Access" measures economic and infrastructural limitations on access to the internet, factors that affect the diversity of internet providers, and the regulatory bodies in the countries. The second category called "Limits on Content" asks questions related to the influence of various actors over censorship and filtering the content, self-censorship, and the level of the internet use as a tool for civic mobilization by the different groups in the country. The last one is called Violation of Users Rights. It examines surveillance, the right to privacy, freedom of online speech, information, and activities.

3.1. The US

National Cyber Strategy of the United States of America (*National Cyber Strategy of the United States of America*, 2018, p. 1) explains how the Trump administration will provide homeland security by protecting networks, systems, functions, and data; promote American prosperity by the protection of economy and empowering domestic innovation; protect peace and security by fostering the Unites States' influence in both domestic and international cyberspace against malicious purposes.

The strategy defines cybersecurity as the protection of components in cyberspace and these components are America's financial, social, government, and political life in a broad sense (*National Cyber Strategy of the United States of America*, 2018, p. 1). According to the National Cyber Strategy (2018), the securitizing actor is the Trump administration and the administration aims to involve other actors –civil society, like-minded states, Federal Government, and private companies- in the securitization of cyberspace. For example, the Federal government is responsible for the protection of federal information systems and national security systems (*National Cyber Strategy of the United States of America*, 2018, p. 6).

The strategy points out some state and non-state actors as threats to security. State actors (Russia, Iran, and North Korea) and non-state actors (terrorists and criminals) are as threats in cyberspace. The US strategy states that Russia, China, Iran, and North Korea attack on the American economy and democracy via cyber tools (*National Cyber Strategy of the United States of America*, 2018, p. 2).

The Strategy prioritizes the security of various referent objects. "Protecting the American people, the American way of life, and American interests are at the forefront of the National Security Strategy" (*National Cyber Strategy of the United States of America*, 2018, p. 6). The strategy repeatedly refers to the term "American people" or "Americans" which represents the citizens of the USA. The referent object is the citizens of America. According to the US strategy, critical cyber infrastructure, federal networks, and information need to be secured for the protection of US citizens. In addition, the US strategy aims to protect American values such as individual liberty, free expression, free markets, and privacy and these objects are linked to the protection of American citizens

or the national security of America (*National Cyber Strategy of the United States of America,* 2018, p. 2).

According to the US strategy, methods to secure cyberspace consist increasing technical capacity, developing cyber technologies, law-making, new policies, standards, and directives. "Securing cyberspace is fundamental to our strategy and requires technical advancements and administrative efficiency across the Federal Government and the private sector" (*National Cyber Strategy of the United States of America*, 2018, p. 2). The Trump administration leads the private sector and the Federal Government to secure critical infrastructure via priority actions. Those actions are the refinement of roles and responsibilities from the Administration, prioritizing actions according to identified national risks, leveraging information and communications technology providers as cybersecurity enablers, protection of democracy, prioritizing national research and development, improvements of transportation, and maritime cybersecurity, and improvement of space cybersecurity. Other determining ways for combatting cybercrime is the modernization of electronic surveillance via the law enforcement and empowering partner nations' law enforcement capacity.

According to "Freedom on the Net 2019 – USA report", the United States has obtained a free state status that is graded as 77 out of 100. "Scores are based on a scale of 0 (least free) to 100 (most free)" (*United States | Freedom House: Freedom on the Net,* 2019). In line with categories that classified in the report, United States' "Obstacle to Access" score is 21 out of 25, "Limits on Content" score is 31 out of 35, and "Violations of User Rights" is 25 out 40. The report states that Internet freedom in the United States has

regularly decreased for the third consecutive year (*United States | Freedom House: Freedom on the Net*, 2019).

Personal data generated especially by immigrants and travelers are stated as a threat to security because security agencies collects personal data because of security concerns. The report *With Liberty to Monitor All* is published by Human Rights Watch in 2014 and it was quoted in the Freedom on the Net 2019 USA report. HRW's report (*With Liberty to Monitor All*, 2014) states that security agencies surveil individuals and collect personal data for national security reasons.

The Report (*United States | Freedom House: Freedom on the Net*, 2019) shows that national security is prioritized in the securitization of cyberspace governance process. Under the category "Violations of User Right", Freedom on the Net USA 2019 report asks the following question "Does the government place restrictions on anonymous communication of encryption" ("United States | Freedom House: Freedom on the Net," 2019).The US has obtained 3 points out of 4 from this part. One of the reasons is about undermining encryption that protect personal data because of national security concerns. The report indicates some cases that show the government's eagerness to undermine encryption. According to the 2019 Report on the US "The government obtained a court order that would have compelled Apple to create new software enabling the FBI to access the phone".

According to the Human Rights Watch's report (*With Liberty to Monitor All*, 2014), the US especially intelligence agencies support large scale surveillance programs to protect the US national security and they aim to get the full authority to collect personal data via surveillance tools. Government agencies and local law enforcement agencies surveil

individuals in the US especially immigrants and visa applicants because of national security measures. Department of Homeland Security and local police departments are examples of agencies. The report (2019) states that “The legal framework for government surveillance has been open to abuse”. The legal framework is usually based on the USA Patriot Act.

The US uses several methods to secure cyberspace governance. The report asks “Does state surveillance of internet activities infringe on users’ right to privacy?”. The US has obtained 2 points out of 6 from this part and this part demonstrates one of the lowest percentages among other parts of the report. The main reason for this lower grade is increasing government-based surveillance (*United States | Freedom House: Freedom on the Net*, 2019). Monitoring social media is one of the most used method of surveillance. Department of Homeland Security collects a vast amount of social media information from travelers, including Americans, and monitoring is not only limited to the individuals; their families, friends, business associates, social media contacts are also surveilled (Patel et al., 2019, p. 6). DHS uses automated tools to monitor social media and it aims to get more authority for the collection of more personal data (Patel et al., 2019, pp. 7–8). In addition to automated tools to monitor individuals, Some of the police departments use fake Facebook accounts to monitor individuals (Maass, 2018).

Section 702 of the FISA Amendments Act of 2008 allows collection of users’ communication data that produced by foreign citizens outside the United States by the National Security Agency (NSA) but Americans’ communication data is also collected/stored (*United States | Freedom House: Freedom on the Net*, 2019).

Executive Order 12333 regulates the reasons and the time for surveillance on individuals in the USA by the NSA or other agencies but it is not clear and transparent enough to balance right to privacy and security measures (*United States | Freedom House: Freedom on the Net*, 2019). According to Freedom on the Net 2019 USA report, the FBI obtains personal data because of national security reasons despite the transparency goal while collecting personal data which is mentioned in the USA Freedom Act. Electronic Frontier Foundation indicates that the USA Freedom Act does not put special attention on Section 702 of the FISA Amendments Act that leads to mass surveillance by security agencies and this act has to put more regulations on to end untargeted surveillance of innocent individuals (Jaycox & Reitman, 2015).

3.2. China

National Cyberspace Security Strategy of China portrayed cybersecurity to promote "comprehensive construction of a well-off society, comprehensively deepen reforms, comprehensively ruling the country according to law, and comprehensively and strictly manage the party's strategic layout" (*National Cyberspace Security Strategy - China*, 2016). The schema of the China's cybersecurity were structured with the pros and cons of cyberspace, its relation with the common interest of humankind.

While explaining cybersecurity strategies, the Chinese government emphasizes cyberspace opportunities and challenges. The challenges can be defined as the sources of the main threats that the Chinese government foresees. The Internet humor, decadent culture, superstitions, and harmful information are the main threats in cyberspace (National Cyberspace Security Strategy - China, 2016). Also, it is stated that the abuse of networks like network monitoring and theft considered a danger for the political

system of China and the other countries (*National Cyberspace Security Strategy - China*, 2016). In addition, the dangerous use of network and information systems to attack the main infrastructures such as finance is another threat in cyberspace. The strategy document identifies terrorists, separatists, and extremists as enemies. Independent hackers also portrayed as the forces who had a detrimental influence on cyberspace security.

China mainly prioritizes cultural security to secure the core values of the society and the value orientations of society. The security of political stability, social order, and network systems are also stated in China's cybersecurity strategy. Moreover, the security of the Communist Party of China has prioritized and cybersecurity is a substantial factor in the management of the party's strategic layout (*National Cyberspace Security Strategy - China*, 2016).

Transparency and openness highlighted as substantial values for the development of such policies. "The public's right to know, participation, expression, and supervision in the cyberspace are fully protected, and the privacy of cyberspace is effectively protected and human rights are fully respected" (*National Cyberspace Security Strategy - China*, 2016).

Several methods to secure cyberspace are stated in the Chines national cybersecurity strategy. The measures that the Chinese government defined in the cybersecurity strategy are taking necessary steps to secure the critical information to hinder data leakages, securing the key information structures via strengthening risk assessment and security protection of key sector, securing culture security via implementing network content construction projects and cracking down on illegal and harmful information

("such as rumors, obscenity, violence, superstition, and cults in the cyberspace"), enhancing the capabilities to fight cyber terror and illegal crime via anti-spyware, improving network governance systems via the formulation of laws and regulations on cybersecurity and supporting the network security research (*National Cyberspace Security Strategy - China*, 2016).

While explaining the goals of its cybersecurity strategy, the strategy document highlights the importance of cooperation amount states. International cooperation is one of methods to secure cyberspace. The Chinese government defines itself as the safeguard of China's cyberspace sovereignty. The government is responsible for taking necessary actions via preventing, punishing, and stopping the defined threat sources. While explaining specific strategies like in network governance terms, the government aims to involve domestic actor to the securitization of cyberspace. It is asserted that "Encourages social organizations to participate in network governance and encourage to report cyber violations and bad information" (*National Cyberspace Security Strategy - China*, 2016).

According to Freedom on the Net 2017, 2018, and 2019 – China reports, China has obtained a "not-free" status that is graded as 12 out of 100 as an average of these three reports. "Scores are based on a scale of 0 (least free) to 100 (most free)" (FON China, 2019, p.1). In line with the categories that classified in the report, China's "Obstacle to Access" score is 8 out of 25, "Limits on Content" score is around 4 out of 35, and "Violations of User Rights" is 0 out 40. The biggest share is based on violations of the user rights category. The score of China is the lowest as compared to other states has reported by Freedom House.

Content providers who express a critical opinion about Chinese Communist Party rule, especially, activists, democracy advocators, minorities, and opposition groups, are restricted or completely prohibited by the government (*China | Freedom House: Freedom on the Net*, 2017; 2018; 2019). Reports (2017; 2018). These content providers can be detained or punished because they are defined as threats to "national security". Activists, democracy advocators, minorities, and opposition groups are threats to security.

"The Chinese government maintains the world's most sophisticated internet censorship apparatus, known informally as the Great Firewall" ("China | Freedom House: Freedom on the Net,", 2017; 2018).The censored topics by the Chinese government are online content about party officials, government policies, and the one-party system ("China | Freedom House: Freedom on the Net,", 2017; 2018;). International news especially about Chinese domestic problems such as corruption and non-democratic policies are the other frequently censored topics. Some social media accounts were deleted and websites were closed because of spreading information that possibly harms the Chinese nation's image and history of the Chinese Communist Party (*China | Freedom House: Freedom on the Net*, 2017). As a current trend, the news and contents about the slowing down of Chinese economic development because of the trade war between the USA and China is the most censored topic in 2019 (*China | Freedom House: Freedom on the Net*, 2019).

Online content manipulation and disinformation are widespread strategies used by Chinese government to control information flow in cyberspace(*China | Freedom House: Freedom on the Net*, 2018). The government encourages social media users to manipulate online content, the reasons are the domination of cyberspace by the

government and sustaining the government's stability in cyberspace ("China | Freedom House: Freedom on the Net,", 2017; 2019). According to the report in 2017, the government supplies financial support to these social media users. The report states that, besides financial support, some of the users are just motivated by ideological reasons (*China | Freedom House: Freedom on the Net*, 2019).

China uses several methods to secure cyberspace. The overall grade of China is decreased from 2017 to 2019. According to the Freedom on the Net report "Conditions for internet users in China continued to deteriorate, confirming the country's status as the world's worst abuser of internet freedom for the fourth consecutive year" (*China | Freedom House: Freedom on the Net*, 2019). The report states that the number of detained or imprisoned Chinese citizens is increasing because of their online sharing and the state controls cyberspace via advanced surveillance tools (*China | Freedom House: Freedom on the Net*, 2019).

Activists and reporters who published online content about pro-democracy, multi-party politics, human rights violations, individual freedoms, right to privacy and freedom of opinion are faced with harsh penalties such as imprisonment in China. Lu Gensong, Chen Shuqing, Sun Feng, Lu Tuyu, Li Tingyu, Liu Feiyu, Huang Qi, Wang Wei, Sun Desheng are just some the activist and reporters who are imprisoned or punished by the state because of online content sharing. ("China | Freedom House: Freedom on the Net,", 2017; 2019).

China's global internet connectivity is controlled by nine state owned operators and operators have right to cut or restrict internet connection of Chinese citizens ("China | Freedom House: Freedom on the Net,", 2017; 2018; 2019). "All service providers must

subscribe via the gateway operators overseen by the Ministry of Industry and Information Technology (MIIT)" (*China | Freedom House: Freedom on the Net*, 2017). As an example of the Internet restriction and shutdown, the contents of ethnic violence against Uyghurs are prohibited by the Chinese government ("China | Freedom House: Freedom on the Net,", 2017; 2018; 2019).

The Internet regulation authorities are a part of or under the control of state institutions and the CCP and the highest regulatory bodies on Internet policy-making is directly led by Xi Jinping ("China | Freedom House: Freedom on the Net,", 2017; 2018; 2019). These regulatory bodies are The State Information Office, Cyberspace Administration office, and Office of the Central Leading Group for Cyberspace Affairs. Internet-based television, online videos, and streaming services are under the control of the State Administration of Radio, Film, and Television (SARFT) and the General Administration for Press and Publications (GAPP) ("China | Freedom House: Freedom on the Net,", 2017; 2018; 2019). According to the Report in 2017, Censorship is one of the regulatory actions which is used frequently by these two bodies. Freedom on the Net 2018 report states that

> Growing censorship demands, new licensing requirements, and data localization mandates under the cybersecurity law that took effect in 2017 have all increased the operational costs of running an internet company in China. Onerous regulations have also hindered the ability of independent media and individual bloggers, journalists, and writers to sustain themselves financially (FoN, 2018, 9)

It means that information sharing by individuals and private companies got complicated and by the Chinese government.

According to the Report published in 2017, "Several social media and messaging apps are totally blocked, isolating the Chinese public from global networks" (*China |*

Freedom House: Freedom on the Net, 2017). YouTube, Google, WhatsApp, Facebook, Pinterest and WordPress are some of the prohibited websites and applications in China.

The freedom of opinion, speech, assembly, association, and publication is protected by article 35 of the Chinese constitution but the judiciary is not independent and protects the CCP's interest ("China | Freedom House: Freedom on the Net,", 2017; 2018; 2019). In 2017, the new cybersecurity law is enacted. The law empowers the authority of security agencies to collect online user's data and to transfer user's data from private websites and companies to security agencies ("China | Freedom House: Freedom on the Net,", 2017; 2019). According to the report, in 2019, developing surveillance technologies and expanding access to user data by security services has led to an increase in arrests and prosecutions.

"Companies offering web services are required to register users, compromising user anonymity and placing user communications at risk of direct government surveillance" (FoN, 2018). Online users have to provide their real names while registering a website or social media applications and service providers are obliged to share user's data with security and intelligence services upon request of agencies ("China | Freedom House: Freedom on the Net,", 2017; 2018; 2019). According to Freedom on the Net - China report (2018; 2019), "The authorities justify real-name registration as a means to prevent cybercrime". Face recognition systems, social media monitoring, and private chat access are frequently used surveillance methods by Chinese security and intelligence agencies, and laws regarding this topic do not restrict these agencies.

3.3. Iceland

Icelandic National Cyber Security Strategy 2015–2026: Plan of action 2015-2018 regulates the use of the Internet and information technology. It was published by the Ministry of Interior in June 2015. The strategy lists four main aims; capacity building, increased resilience, strengthened legislation and tackling cybercrime.

In the strategy paper, cybersecurity is defined as the protection of physical infrastructure and economic prosperity from the cyber threats while respecting the right to privacy and individual freedoms. The key securing actor is the Ministry of the Interior and it is responsible for the formulation of government strategy of cybersecurity and the protection of physical infrastructure in cyberspace which is relevant to national security.

Criminal organisations defined as a threat to cybersecurity. The strategy aims to prevent activities of criminal organisations via strengthening the cybersecurity measures because low level of cybersecurity makes Iceland vulnerable to "Cybercrime", "digital espionage", and "the abuse of personal and commercial data" (*Icelandic National Cyber Security Strategy 2015-2026 Plan of Action 2015-2018*, 2015).

The right to privacy is a core value and has to be respected while securing cyberspace. While securing cyberspace "Icelandic legislation should reflect the international demands and obligations the country undertakes regarding cybersecurity and the protection of personal data" (*Icelandic National Cyber Security Strategy 2015-2026 Plan of Action 2015-2018,* 2015). European Union, European Commission, and NATO can classify some demand and concerns relevant to cybersecurity. Economy is also defined as vulnerable to threats in cyberspace such as industrial espionage (*Icelandic*

National Cyber Security Strategy 2015-2026 Plan of Action 2015-2018, 2015). Referent objects are economy, individual freedoms, right to privacy, and physical infrastructure.

The main methods to secure cyberspace are capacity building, increased resilience, strengthened legislation, and tackling cybercrime. (*Icelandic National Cyber Security Strategy 2015-2026 Plan of Action 2015-2018*, 2015).

"Capacity Building" measures are awareness-raising, terminology, education, postgraduate studies, design values, and personal data protection. Awareness-raising consist of increasing knowledge and cooperation on cybersecurity issues among actors in the state especially the public, enterprises, and government ("Iceland | Freedom House: Freedom on the Net," 2019). Terminology means the creation of an Icelandic translation of main terms in cybersecurity terminology. According to the education method, cybersecurity topic has to involve all computer-related studies to increase knowledge and expertise on this topic. Design values define secure cyberspace and personal data protection as two main values. Finally, the personal data protection method includes that cybersecurity measures have to be respectful to international standards and obligations with respect to personal data ("Iceland | Freedom House: Freedom on the Net," 2019).

Key "Increased resilience" methods are international collaboration and reliability of primary data systems. International collaboration consist of increasing Iceland's involvement in cybersecurity abroad. Reliability of primary data systems means that telecommunications systems and the primary data transmission systems have to be supportive to the security of cyberspace with reliable data.

According to Freedom on the Net reports on Iceland, Iceland got the highest score among other countries in the report for 4 consecutive years (*Iceland | Freedom House: Freedom on the Net*, 2019). Iceland has obtained a "free state" status with averagely 94 out of 100. In line with categories that classified in reports, the mean scores for Iceland (based on four annual reports) are "Obstacle to Access" score is 24,5 out of 25, "Limits on Content" score is 34 out of 35, and "Violations of User Rights" is 35,75 out 40.

According to the 2016 Iceland report, Icelandic society is strongly engaged with the internet and the digital world and Iceland is the top promoter of free speech. According to the 2017 report, "...84 percent of individuals used social networks, 95 percent read news online, 95 percent sent or received emails, 36 percent stored electronic content online, and 66 percent used internet commerce" (*Iceland | Freedom House: Freedom on the Net*, 2017).

Three threats in cyberspace governance are stated in Freedom on the Net Iceland report. The first threat is the collection of personal data as against to right to privacy of citizens of Iceland by allied intelligence agencies (United Kingdom, Australia, Canada, and New Zealand) especially by the US and the UK. According to the report, users data on online communication had been collected by allied intelligence agencies and the Government of Iceland was unable to protect the right to privacy of its citizens against surveillance made by allied intelligence agencies ("Iceland | Freedom House: Freedom on the Net," 2018; 2019). Cyberattacks are the second threat in cyberspace. "In October 2018, Iceland experienced one of its largest cyberattacks, with thousands of users receiving sophisticated phishing emails that prompted them to download malware from a bogus website impersonating that of the national police" ("Iceland | Freedom House: Freedom

on the Net," 2019). As a consequence of the cyber-attack in 2018, hundreds of data about users' bank account were stolen. Online discrimination against the "nationality, color, race, religion, sexual orientation or gender identity" of a person is the third threat in cyberspace. ("Iceland | Freedom House: Freedom on the Net," 2018; 2019).

The security of right to privacy is prioritized in Iceland while securing cyberspace governance. The right to privacy is protected by strong legal regulations and policies (*Iceland | Freedom House: Freedom on the Net*, 2016; 2017; 2018; 2019). The report in 2019 states that "Users are generally free from state surveillance, which is regulated under the Telecommunications Law" (*Iceland | Freedom House: Freedom on the Net*, 2019).

Iceland follows three main methods against threats in cyberspace. "Increase Resilience", "Strengthen Legislation", and "International cooperation" are three main methods to secure cyberspace. These methods are defined in cybersecurity strategy paper of Iceland published in 2015. "In 2015, the Ministry of the Interior published an ICT security policy that aimed to increase resilience to, raise awareness about, and expand collaboration with international organizations on cybersecurity issues" (*Iceland | Freedom House: Freedom on the Net*, 2019).

CHAPTER IV

ANALYSIS AND CONCLUSION

This chapter presents two types of comparisons. Within-case comparison for each country is the first type. The thesis compares two types of data offered by the national cybersecurity strategies and Freedom on the Net reports. Two types of data represent two schemas of securitization of cyberspace governance. The national cybersecurity strategy papers reflect how states portray their own schema of the securitization of cyberspace governance. On the other hand, Freedom on the Net reports examine how do selected countries securitize cyberspace governance in practice. The second type of comparison is each state with the other based on the findings achieved via within-case comparisons.

When the cybersecurity strategy published by the American government in 2018 is analyzed, cybersecurity is defined as the protection of America's financial, social, governmental, and political life (*National Cyber Strategy of the United States of America,* 2018). Cybersecurity is presented as a requirement to protect these four broad referents. Two different threats to security in cyberspace are identified. The first is defined as state actors, especially Russia, Iran, and North Korea, while the second is defined as non-state actors, including terrorists, hackers, and criminals (*National Cyber Strategy of the United States of America,* 2018). Cybersecurity is presented as a

necessity for the protection of America's financial, social, governance, and political life, and the main reason for protecting these four is to ensure the security of the American people. At this point, priority is given to the security of the American people from state and non-state threat actors in cyberspace. In order to secure the American people against threats in cyberspace, the main methods to secure are followed to increase the technical capacity related to cyberspace and to introduce new laws, policies, and regulations (*National Cyber Strategy of the United States of America*, 2018).

When Freedom on the Net US reports published by Freedom House in 2019 are examined, the American government, especially security agencies such as the Department of Homeland Security, define personal data as a threat to national security in cyberspace. The purpose of monitoring personal data is to eliminate possible threats to national security in cyberspace. In this context, the US government prioritize the protection of national security in cyberspace. The government use various methods for the protection of national security. These methods are social media monitoring and government base surveillance (*United States | Freedom House: Freedom on the Net*, 2019).

There are two different schemas of the securitization of cyberspace governance in the US. These two schemas answer "How does the US securitize cyberspace governance based on two different data?". The first schema is created by the analysis of the US cybersecurity strategy paper. Accordingly, The US government claims to create secure cyberspace for the American people. However, the second schema that is created by the analysis of Freedom on the Net US report presents a different approach for the securitization of cyberspace governance. The second schema is the outcome of actions

made by the US government to create a more secure cyberspace. According to the second schema, it is clear that the US government surveil individuals both US citizens and immigrants in the US because of national security purposes. The government directly violates the right to privacy of individuals in the US. Surveillance tools mostly used by security agencies and securing the national security of the US does not secure the American people and especially the right to privacy of the American people. It means that the securitization of cyberspace governance is not compatible with the right to privacy in the US. The US is a free and democratic state but takes non-democratic measures such as surveillance as a method to securitize cyberspace governance. What the government declares to do is in tension with its practices.

TABLE 1. TWO SCHEMAS FOR THE SECURITIZATION OF CYBERSPACE GOVERNANCE IN THE US

	The US	
	Strategy Paper	**Freedom on the Net Reports**
Grade	N/A	Status - Free Obstacle to Access - 21 out of 25 Limits on Content - 31 out of 35 Violations of User Rights - 25 out 40
What is the definition of security?	The protection of America's financial, social, government, and political life	N/A
What / Who are threats to security?	State actors (Russia, Iran, North Korea) and Non-state actors (Cyber Criminals)	Personal Data
What / Who is being secured?	American People	National Security
How is security addressed?	Increasing Technical, Legal, and Administrative Capacity	Surveillance

When the cybersecurity strategy published by the Chinese Government in 2016 is examined, a very broad definition for cybersecurity emerges. Cybersecurity is associated

with the well-being of society, rule of law, and the strategic layout of the Chinese Communist Party. The strategy paper specifies some of the threats that emerge in cyberspace. These threats are “the Internet humor”, “decadent culture”, and “harmful information”. “Terrorists”, “separatists”, and “extremists” are defined as actors posing threats in cyberspace. Against these threats and threats sources, the security of the culture, the nation, the political stability, and most importantly, the Chinese Communist Party are prioritized. Different methods are highlighted in the strategy paper to protect referent objects. These methods are to increase technical capacity in cyberspace, to construct content for cyberspace by the government, to prevent illegal and harmful information, to make laws and regulations, and to ensure international cooperation.

When Freedom on the Net China reports published in 2017, 2018, and 2019 are analyzed, it is seen that activists, democracy advocators, minorities, and opposition groups are threats in cyberspace. Against these actors, who are stated as threats in cyberspace, the security of the Chinese Communist Party is prioritized. This means that the referent object is the Chinese Communist Party. Against these threats, the government takes different measures. These measures are detainment, the Internet restriction, censorship, content manipulation and disinformation, surveillance, social media monitoring.

Two schemas regarding the case of China answer “How does China securitize cyberspace governance based on two different data?”. When two schemas sourced by the cybersecurity strategy paper published by the Chinese Government and Freedom on the Net China reports are compared, it seems that cybersecurity is only defined in the cybersecurity strategy paper. Cybersecurity is defined in the strategy report as a broad

concept that can have an impact on every field. Examples of these fields are the well-being of society, rule of law, following regulations made by the Communist Party. The Chinese state identifies separatists and extremists as threats in the securitization of the cyberspace governance process. According to the Freedom on the Net China report, opposition groups such as activists, democracy advocates, and minorities are stated as security threats in the securitization of cyberspace governance process. The Chinese state prioritizes the security of Chinese culture, political stability, social order, and especially the Chinese Communist Party in its strategy paper. The Freedom on the Net report, on the other hand, states that the security of the Chinese Communist Party is prioritized accordingly. When comparing the methods of providing security, the Chinese state states that it will use methods that increase technical, legal, and international cooperation capacity. In contrast, the Freedom on the Net China report states that detainment, censorship, and surveillance are methods widely used to provide security.

China as a not-free and undemocratic state follows non-democratic measures for the securitization of cyberspace governance. The government aims to suppress opposition to the Chinese Communist Party with censorship and surveillance. The right to privacy is harshly violated and the government has the legal right to control personal data. What the Chinese state declared in the strategy paper and the real actions for the securitization are more compatible with each other when compared to the US. It means that two schemas created by the analysis of the Chinese cybersecurity strategy paper and Freedom on the Net China reports present similarities and dissimilarities at the same time.

TABLE 2. TWO SCHEMAS FOR THE SECURITIZATION OF CYBERSPACE GOVERNANCE IN CHINA

	China	
	Strategy Paper	**Freedom on the Net Reports**
Grade	N/A	Status - Not Free Obstacle to Access - 8 out of 25 Limits on Content - 4 out of 35 Violations of User Rights - 0 out 40
What is the definition of security?	"Cybersecurity stated as an important measure to coordinate and promote the comprehensive construction of a well-off society, comprehensively deepen reforms, comprehensively ruling the country according to law, and comprehensively and strictly manage the party's strategic layout."	N/A
What / Who are threats to security?	Harmful Content and Misinformation / Cyber Criminals and Opposition Groups	Opposition Groups
What / Who is being secured?	Culture, Nation, Chinese Communist Party	Chinese Communist Party
How is security addressed?	Increasing Technical, Legal, Administrative, and International Cooperation Capacity	Censorship, Disinformation, and Surveillance

When the Iceland cybersecurity strategy paper published in 2015 is examined, it is emphasized that the physical infrastructure and economic prosperity have to be secured,

and the right to privacy should be respected while securing cyberspace. In cyberspace, cybercrime, digital espionage, and the abuse of personal and commercial data are defined as security threats, and criminal organizations are defined as actors that cause threats. Economy, individual freedoms, and the right to privacy is defined as referent objects that need to be secured primarily. In order to secure these reference objects, increasing technical capacity, strengthen legislation, international cooperation methods are applied.

When the Freedom on the Net Iceland reports published in 2016, 2017, 2018, and 2019 are examined, foreign intelligence agencies come to the fore as the actors posing a threat in cyberspace, and cyberattacks are threats. The security of the right to privacy as a referent object is prioritized. Increasing the technical capacity, strengthening the laws and international cooperation methods are preferred in order to secure the right to privacy.

Dunn Cavelty (2008) states that the lack of extraordinary measures against threats and risks in cyberspace is examined as a case of failed securitization. When the Iceland case is considered, there are not any extraordinary measures to secure cyberspace governance. However, Eriksson (2001) excludes extraordinary measures from the securitization process and states that extraordinary measures are not obligatory for a successful securitization of cyberspace, political actors can take ordinary measures derived from normal politics against threats. From Eriksson's (2001) point of view, Iceland securitizes cyberspace governance without extraordinary measures. Therefore, the Iceland case challenges the necessity of extraordinary measures in the securitization of cyberspace governance.

When two different schemas sourced by the strategy paper published by the Icelandic government and Freedom on the Net Iceland reports are compared in terms of threats, referent objects, and securitization methods, answers to the mains questions are consistent with each other. For example, in the Strategy report, the violation of personal privacy is defined as a preliminary threat, while in the Freedom on the Net report, abuse of the right to privacy due to the violation of personal data by foreign intelligence agencies is a threat.

Iceland as a free and democratic state follows a democratic approach for the securitization of cyberspace governance. The government aims to keep a balance between the right to privacy and the security of physical infrastructure and economic prosperity. What the Icelandic government declared in the strategy paper and the real actions are more compatible with each other when compared to the US and China. It means that two schemas created by the analysis of the Icelandic cybersecurity strategy paper and Freedom on the Net Iceland report are mostly similar to each other.

TABLE 3. TWO SCHEMAS FOR THE SECURITIZATION OF CYBERSPACE GOVERNANCE IN ICELAND

	Iceland	
	Strategy Paper	**Freedom on the Net Reports**
Grade	N/A	Status - Free Obstacle to Access - 24,5 out of 25 Limits on Content - 34 out of 35 Violations of User Rights - 36 out 40
What is the definition of security?	The protection of physical infrastructure and economic prosperity from cyber threats while respecting the right to privacy and individual freedoms	N/A
What / Who are threats to security?	Cyber Criminals	Foreign Intelligence Agencies and Cyber Criminals
What / Who is being secured?	Economic Prosperity, Individual Freedoms, Right to Privacy	Right to Privacy
How is security addressed?	Increasing Technical, Legal, Administrative, and International Cooperation Capacity	Increasing Technical, Legal, Administrative, and International Cooperation Capacity

The US and Iceland as both free and democratic states follow different approaches in the securitization of cyberspace governance. The US government employs undemocratic measures such as surveillance and violates the right to privacy to provide security.

However, the Icelandic government aims to take security measures that are compatible with the right to privacy as different from the US. China as a not-free and non-democratic state follows a non-democratic approach in the securitization of cyberspace governance and violates the right to privacy. Taking security measures as compatible with the right to privacy is not prioritized by the Chinese government. The main concern is regime security as maintained by the Chinese Communist Party.

This thesis observes a complicated relationship between the securitization of cyberspace governance and the right to privacy. What governments declare and their practices can be inconsistent as in the US, can be consistent as in Iceland, and can be consistent and inconsistent at the same time as in China. The level of democracy cannot guarantee the adoption of democratic measures to secure cyberspace governance. Democratic and undemocratic states can take the same measures such as surveillance to secure cyberspace governance, but also a democratic state can take democratic measures to secure cyberspace governance.

TABLE 4. THREE APPROACHES TO THE SECURITIZATION OF CYBERSPACE GOVERNANCE

	National Security-Centric Approach	**Regime Security-Centric Approach**	**Individual Security-Centric Approach**
What / Who are threats to security?	Personal Data	Opposition Groups	Abuse of Data
What / Who is being secured?	National Security	Authority	Right to Privacy
How is security addressed?	Non-Democratic Measures	Non-Democratic Measures	Democratic Measures

When the three cases are compared with each other, three main approaches become visible regarding the securitization of cyberspace governance. These approaches are derived from the application of the securitization theory to the study of cyberspace governance. Approaches can be applied not only in three cases in this thesis but also to other countries. In addition, a case does not have to fit into only one approach, some cases can show similar specifications with two or three of these approaches.

The first approach places national security as the main referent object of securitization.

The national security-centric approach perceive personal data as a threat to the referent object. Security agencies aim to collect and process personal data to deal with threats against national security. The agencies take non-democratic measures without public accountability and transparency such as surveillance and social media monitoring to collect personal data.

Security measures are raised and some individual freedoms are sacrificed in the name of the "right" balance. Bigo (2012, p. 277)

> Individuals, the city, the nation, the planet, depending on the scale of the danger, need to be protected by security measures in order to survive. Moreover, the state's duty to protect implies that it must act efficiently, not only to detect those responsible after an act of violence, but also to respond at the time, and more importantly, beforehand, so that violence may be prevented. In order to act in this way, the state and its agencies need to gather, store, analyze and apply as much information as possible. This dominant narrative assumes also that the more information is gathered by the state, and in a timely way, the greater the level of security is offered to it and its citizens.

Security agencies advocate that collecting a vast amount of personal data enables forecasting threats to national security before the real threat occurs. It means that national security comes first then the right to privacy. The US case follows national security-centric approach.

The second approach places the regime as the main referent object of securitization. The regime security-centric approach perceives opposition to authority as a threat to the referent object. The opposition groups can be ethnic or religious minorities and extremist. In order to protect the regime, political actors can take non-democratic measures such as detainment, censorship, and misinformation. The regime can be a political party, the ruling class, and a dictator. The case of China represents an example of regime security-centric approach.

Individual security-centric approach prioritizes the security of the right to privacy. Democratic measures such as strict data regulations are a way to protect the right to privacy. The main threat is understood as the collection of private and commercial data by state actors such as foreign intelligence agencies and non-state actors such as cybercriminals. Iceland has put individual security-centric approach to the core to secure cyberspace governance.

Three approaches demonstrate that securitizing actors have two main options while securing cyberspace governance. The first option is the securitization of cyberspace governance in a way that is compatible with the right to privacy. The second option is prioritizing other referent objects such as national security or the regime while infringing upon the right to privacy.

Actors who aim to secure cyberspace also present dichotomous choices to citizens. "The assumption is that citizens will happily give information in order that they enjoy the pleasure of being securitized, to be protected by a group of professionals in charge of security"(Bigo, 2012, p. 277). Therefore, citizens have to choose between two options. The first one is being not secured against threats in cyberspace and the second one sharing personal data with security providers to be secured. According to this dichotomous situation, audience and securitizing actors are already assumed to have agreed that a certain issue can be defined as a security threat and there is a need for exceptional measures such as surveillance. Dichotomous choices exclude audience response from the securitization equation.

Conclusion

To conclude, I adopted securitization theory in the study of cyberspace governance to understand how various states securitize cyberspace governance and analyze how various schemas in the securitization of cyberspace governance affect the right to privacy. States securitize cyberspace governance because cyberspace consists of thousands of threats and fragilities at the same time. The critical point here is the methods to provide security in cyberspace.

To understand various schemas of the securitization of cyberspace governance, I looked for answers in data to 4 main questions derived from the securitization theory. I selected 3 cases as the US, China, and Iceland. For each case, I analyzed two types of public data. The first data is cybersecurity strategy papers that are published by the government of the selected case and freedom on the net reports that are published by Freedom House. Each case brings two different schemas for the securitization of cyberspace governance based on the data type. I make within-case comparisons for each case and also I make inter case comparisons.

For the purpose of within-case comparison, when different schemes of securitization of cyberspace governance are examined for each case, the compatibility of what countries declare in their strategy papers and what they actually implement based on freedom on the net reports is analyzed. In order to analyze the compatibility, 4 main questions sourced by the securitization theory were answered by examining the aforementioned sources. This thesis demonstrates that two different schemes created for each country can be compatible, incompatible, and both compatible and incompatible simultaneously. The findings reached as a result of the analysis of within-case and inter-case

comparisons are explained below.

Firstly, when the US case was analyzed, incompatibilities were observed between what did the US government declare and what was actually implemented for the securitization of cyberspace governance. On the other hand, when the Chinese case was analyzed, it has been reached that what did the Chinese government declare and what was actually implemented for the securitization of cyberspace governance was compatible and incompatible in some instances. Finally, when the Icelandic case was observed, securitization of cyberspace governance based on declaration in the strategy paper and the real-life implementations in the freedom on the net reports were compatible.

In the case of China, the Chinese government stated in the strategy paper that opposing groups were a threat to cybersecurity and according to the freedom on the net reports, the government took various measures such as censorship and detainment against these groups in real-life implementations. The American government defined the main threat in cybersecurity as state actors such as Russia, Iran, and North Korea but the American government perceive personal data as a threat in practice and aimed to obtain personal data through methods such as surveillance. In addition, the Chinese government prioritizes the security of the Chinese Communist Party in its strategy paper, and the measures it takes are parallel to this. However, in the case of America, the government prioritizes the security of the American people according to the cybersecurity strategy paper but it actually prioritized the protection of national security in practice according to the freedom on the net reports. Comparing the case of America and China, the Chinese Government's declaration and real-life applications for the securitization of cyberspace governance are more parallel with each other.

When the Iceland case is examined, the Icelandic government has defined cybercriminals as a threat in the securitization of the cyberspace governance process, and the government's real-life implementations are correspondent with the government's declaration in the cybersecurity strategy paper. In addition, the Icelandic government has prioritized the security of the right to privacy in its strategy paper, and implementation has progressed in parallel. It is aimed to protect personal data with methods such as increasing technical, legal, administrative, and international cooperation capacity. However, when the US case is examined, as mentioned above, differences were observed between the answers to the questions of who/what is being secured and who/what are threats to security. Comparing the case of America and Iceland, the Icelandic Government's declaration for the securitization of cyberspace governance and real-life applications are more in parallel with each other than in America.

According to this thesis, there is a relationship between how states securitize cyberspace governance and the right to privacy. Securitization of cyberspace governance with respect to the right to privacy is too complex. When three cases were analyzed, there is no certain pattern between what the governments declare to the public and results of their actions in real-life in regards to the securitization process.

Based on these comparisons there are two main arguments. According to within-case comparisons, what governments declare to secure cyberspace governance and their real-time actions to secure cyberspace can be similar, different, or partly similar and partly different. When compared to cases with each other, it is seen that a free and not-free state can cause threats to the right to privacy via using surveillance tools because of various security concerns. The level of democracy in a state does not guarantee a

security schema that is compatible with the right to privacy.

There are possible reasons to explain why both the US as a democratic and China as an undemocratic state securitize cyberspace governance. The first reason can be the number of Internet users in the US and China. The number of Internet users in China is the highest in the world and the US is the second. The high number of Internet users means the high number of targets for cybercriminals. China and the US can be the most attacked states in cyberspace. Both states can use the securitization of cyberspace governance as a tool against threats in cyberspace.

As the second reason, the number of threats is unlimited in cyberspace. These threats are digital espionage, hacking attacks, misinformation, data manipulation, and so on. The number of targets is also unlimited in cyberspace. Targets can be Internet users, businesses, states, governments, technological infrastructure, organizations, and so on. All of these targets create fragilities and threat sources as state and non-state actors benefit from this situation. Therefore, both democratic and non-democratic states can securitize cyberspace against these threat sources. So as to respond the sudden threats and fragilities, governments can take extraordinary measures.

In this thesis, there is not a concrete pattern that explains the relationship between the securitization of cyberspace governance and the right to privacy. The reason for this can be the number of cases. For further research, the number of cases can be increased and researchers can use quantitative methods for their analysis. The number of qualitative and quantitative studies that apply securitization theory to the field of cyberspace is too limited.

In the literature, current studies do not explain audience response, extraordinary measures, referent objects in detail and systematically. Especially, the audience response in the securitization of cyberspace governance topic is still blurred. There can be two possible explanations for why audience response disregarded. Cyberspace is a unique field that changes happen suddenly and threats may require abrupt responses. Thus, audience response can delay taking extraordinary measures process. As the second explanation, the audience especially citizens of a state cannot be completely aware of the technical features of cyberspace. The technical details goes beyond the expertise of the audience. This makes the audience response unnecessary in the securitization of cyberspace governance topic. There is a need for further research to test and analyze these for possible reasons.

REFERENCES

About Us | Freedom House. (n.d.). Retrieved September 30, 2020, from https://freedomhouse.org/about-us

Ad'ha Aljunied, S. M. (2019). The securitisation of cyberspace governance in Singapore. *Asian Security*, *00*(00), 1–20.

Anckar, C. (2008). On the applicability of the most similar systems design and the most different systems design in comparative research. *International Journal of Social Research Methodology*, *11*(5), 389–401.

Aradau, C. (2004). Security and the democratic scene: desecuritization and emancipation. *Journal of International Relations and Development*, *7*, 388–413.

Balzacq, T., Léonard, S., & Ruzicka, J. (2016). 'Securitization' revisited: theory and cases. *International Relations*, *30*(4), 494–531.

Barlow, J. P. (1996). *Thinking locally, acting globally | Electronic Frontier Foundation*. https://www.eff.org/pages/thinking-locally-acting-globally

Bauer, J. M. (2005). *Internet Governance: Theory and First Principle*.

Bigo, D. (2002). Security and Immigration: Toward a Critique of the Governmentality of Unease. *Alternatives: Global, Local, Political*, *27*(1), 63–92.

Bigo, D. (2012). Security, surveillance, and democracy. In K. Ball, K. D. Haggerty, & D. Lyon (Eds.), *Routledge Handbook of Surveillance Studies* (pp. 277–285). Routledge.

Blatter, J. K. (2008). Case Study. In L. M. Given (Ed.), *The SAGE Encyclopedia of Qualitative Research Method* (p. 692). SAGE Publications. https://books.google.com/books?id=y_0nAQAAMAAJ&pgis=1

Brown, D., Esterhuysen, A., & Knodel, M. (2012). *Briefing Document: Cybersecurity Policy and Human Rights*. Association for Progressive Communication.

Buzan, B., & Wæver, O. (2009). Macrosecuritisation and Security Constellations: Reconsidering Scale in Securitisation Theory. *Review of International Studies*, *35*(2), 253–276.

Buzan, B., Waever, O., & Wilde, J. de. (1998). *Security: A New Framework for Analysis*. Lynne Rienner Publishers.

China: Freedom in the World 2021 Country Report. (2021). https://freedomhouse.org/country/china/freedom-world/2021

China | Freedom House: Freedom on the Net. (2017). https://freedomhouse.org/country/china/freedom-net/2017

China | Freedom House: Freedom on the Net. (2018). https://freedomhouse.org/country/china/freedom-net/2018

China | Freedom House: Freedom on the Net. (2019). https://freedomhouse.org/country/china/freedom-net/2019

Cyberspace. (n.d.). Retrieved December 24, 2019, from https://www.oed.com/view/Entry/240849?redirectedFrom=cyberspace

De Meur, G., & Berg-Schlosser, D. (1996). Conditions of Authoritarianism, Fascism, and Democracy in Interwar Europe: Systematic Matching and Contrasting of Cases for "Small N" Analysis. *Comparative Political Studies*, *29*(4), 423–468. http://hjb.sagepub.com.proxy.lib.umich.edu/content/9/2/183.full.pdf+html

Deibert, R. J. (2002). Circuits of Power: Security in the Internet Environment. In J. N. Rosenau & J. P. Singh (Eds.), *Information Technlogies and Global Politics: The Changing Scope of Power and Governance* (pp. 115–143). State University of New York Press.

Deibert, R. J. (2018). Toward a Human-Centric Approach to Cybersecurity. *Ethics and International Affairs*, *32*(4), 411–424.

Deibert, R. J., & Crete-Nishihata, M. (2012). Global Governance and the Spread of Cyberspace Control. *Global Governance*, *18*, 339–361.

Deibert, R. J., & Rohozinski, R. (2010a). Control and Subversion in Russian Cyberspace. In R. J. Deibert, J. Palfrey, R. Rohozinski, & J. Zittrain (Eds.), *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* (pp. 15–34). The MIT Press.

Deibert, R. J., & Rohozinski, R. (2010b). Liberation vs. Control: The Future of Cyberspace. *Journal of Democracy*, *21*(4), 43–57. http://muse.jhu.edu/content/crossref/journals/journal_of_democracy/v021/21.4.deibert.html

Deibert, R. J., & Rohozinski, R. (2010c). Risking security: Policies and paradoxes of cyberspace security. *International Political Sociology*, *4*(1), 15–32.

Denardis, L. (2014). *The Global War for Internet Governance*. Yale Universty Press.

Dunn Cavelty, M. (2013). From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse. *International Studies Review*, *15*(1), 105–122.

Dunn Cavelty, M., & Egloff, F. J. (2019). The Politics of Cybersecurity: Balancing Different Roles of the State. *St Antony's International Review*, *15*(1), 37–57.

Eldem, T. (2019). The Governance of Turkey's Cyberspace: Between Cyber Security and Information Security. *International Journal of Public Administration*, *43*(5), 452–465. https://doi.org/10.1080/01900692.2019.1680689

Entman, R. M., & Usher, N. (2018). Framing in a Fractured Democracy: Impacts of Digital Technology on Ideology, Power and Cascading Network Activation. *Journal of Communication*, *68*(2), 298–308.

Fang, B. (2018). Cyberspace Sovereignty. In *Cyberspace Sovereignty: Reflections on building a community of common future in cyberspace*. Springer.

Gerring, J. (2007). *Case Study Research: Principles and Practices*. Cambridge University Press.

Gerring, J., & Cojocaru, L. (2016). Selecting Cases for Intensive Analysis: A Diversity of Goals and Methods. In *Sociological Methods and Research* (Vol. 45, Issue 3).

Gorr, D., & Schünemann, W. J. (2013). Creating a secure cyberspace - Securitization in Internet governance discourses and dispositives in Germany and Russia. *International Review of Information Ethics*, *20*, 37–51.

Gunitsky, S. (2015). Corrupting the cyber-commons: Social media as a tool of autocratic stability. *Perspectives on Politics*, *13*(1), 42–54.

Hancke, B. (2009). *Intelligent Research Design: A guide for beginning researchers in the social sciences*. Oxford University Press.

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the copenhagen school. *International Studies Quarterly*, *53*(4), 1155–1175.

Howard, D. M. (2018). Can Democracy Withstand the Cyber Age: 1984 in the 21st Century. *Hastings Law Journal*, *69*(5), 1355–1378.

Hundley, R. O., & Anderson, R. H. (1997). Emerging Challenge: Security and Safety in Cyberspace. In J. Arquilla & D. Ronfeldt (Eds.), *In Athena's Camp: Preparing for Conflict in the Information Age* (pp. 231–253). RAND. http://books.google.com/books?hl=en&lr=&id=qJGawYmm6b4C&pgis=1

Iceland: Freedom in the World 2021 Country Report. (2021). https://freedomhouse.org/country/iceland/freedom-world/2021

Iceland | Freedom House: Freedom on the Net. (2016). https://freedomhouse.org/country/iceland/freedom-net/2016

Iceland | Freedom House: Freedom on the Net. (2017). https://freedomhouse.org/country/iceland/freedom-net/2017

Iceland | Freedom House: Freedom on the Net. (2018). https://freedomhouse.org/country/iceland/freedom-net/2018

Iceland | Freedom House: Freedom on the Net. (2019). https://freedomhouse.org/country/iceland/freedom-net/2019

Icelandic National Cyber Security Strategy 2015-2026 Plan of Action 2015-2018. (2015). https://www.stjornarradid.is/media/innanrikisraduneyti-media/media/frettir-2015/Icelandic_National_Cyber_Security_Summary_loka.pdf

Internet World Stats. (2021). Usage and Population Statistics. http://www.internetworldstats.com/stats.htm

Jayawardane, S., Larik, J., & Jackson, E. (2015). *Cyber Governance: Challenges, Solutions, and Lessons for Effective Global Governance*.

Jaycox, M., & Reitman, R. (2015). The New USA Freedom Act: A Step in the Right Direction, but More Must Be Done. *Electronic Frontier Foundation*, 1–8. https://www.eff.org/deeplinks/2015/04/new-usa-freedom-act-step-right-direction-more-must-be-done

King, G., Keohane, R. O., & Verba, S. (1994). The Science in Social Science. In *Designing Social Inquiry:scientific inference in qualitative research*. Princeton University Press.

Kingsmith, A. T. (2013). Virtual Roadblocks: The Securitisation of the Information Superhighway. *Bridges: Conversations in Global Politics and Public Policy*, *2*(1), 1–14.

Kobrin, S. J. (2001). Territoriality of Cyberspace. *Journal of International Business Studies*, *32*(4), 687–704.

Kuehl, D. T. (2009). From Cyberspace to Cyberpower. In F. D. Kramer, S. H. Starr, & L. K. Wentz (Eds.), *Cyberpower and National Security* (pp. 24–42). University of Nebraska Press.

Lijphart, A. (1975). The Comparable-Cases Strategy in Comparative Research. *Comparative Political Studies*, *8*(2), 158–177.

Loader, B. D. (1997). The governance of cyberspace: politics, technology and global restructuring. In B. D. Loader (Ed.), *The Governance of Cyberspace* (pp. 1–20). Routledge.

Lobato, L. C., & Kenkel, K. M. (2015). Discourses of cyberspace securitization in Brazil and United States. *Revista Brasileira de Politica Internacional*, *58*(2), 23–43.

Maass, D. (2018). *Facebook Warns Memphis Police: No More Fake "Bob Smith" Accounts*. EFF| Electronic Frontier Foundation. https://www.eff.org/deeplinks/2018/09/facebook-warns-memphis-police-no-more-fake-bob-smith-accounts

Mahoney, J., & Goertz, G. (2006). A tale of two cultures: Contrasting quantitative and qualitative research. *Political Analysis*, *14*, 227–249.

Mathiason, J. (2009). *Internet Governance: The new frontier of global institutions*. Routledge.

Mathiason, J., Mueller, M., Klein, H., Holitscher, M., & McKnight, L. (2004). *Internet governance: state of play*. http://dcc.syr.edu/miscarticles/MainReport-final.pdf

Mueller, M. (2010). *Networks and States The Global Politics of Internet Governance*. The MIT Press.

National Cyber Strategy of the United States of America. (2018). https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

National Cyberspace Security Strategy - China. (2016). http://www.cac.gov.cn/2016-12/27/c_1120195926.htm

Neal, A. W. (2012). Terrorism, Lawmaking, and Democratic Politics: Legislators as security actors. *Terrorism and Political Violence*, *24*(3), 357–374.

Opderbeck, D. W. (2012). Cybersecurity and Executive Power. *Washington University Law Review*, *89*(4), 795–846.

Patel, F., Levinson-Waldman, R., DenUyl, S., & Koreh, R. (2019). *Social Media Monitoring How the Department of Homeland Security Uses Digital Data in the Name of National Security*.

Ramirez, M. J. (2017). Some Criminal Aspects of Cybersecurity. In M. J. Ramirez & L. A. Garcia-Segura (Eds.), *Cyberspace: Risks and Benefits for Society, Security and Development* (pp. 141–153). Springer International Publishing.

Rheingold, H. (1994). *Virtual Community: Homesteading on the Electronic Frontier*. Harper Trade.

Rød, E. G., & Weidmann, N. B. (2015). Empowering activists or autocrats? The Internet in authoritarian regimes. *Journal of Peace Research*, *52*(3), 338–351.

Shackelford, S. J. (2016). Protecting Intellectual Property and Privacy in the Digital Age: The Use of National Cybersecurity Strategies to Mitigate Cyber Risk. *Chapman Law Review*, *19*(2), 445–482.

Shen, F., & Liang, H. (2015). Cultural Difference , Social Values , or Political Systems ? Predicting Willingness to Engage in Online Political Discussion in 75 Societies. *International Journal of Public Opinion Research*, *27*(1), 111–124.

Shen, Y. (2016). Cyber Sovereignty and the Governance of Global Cyberspace. *Chinese Political Science Review*, *1*(1), 81–93.

Skocpol, T. (1979). *States and Social Revolutions: A Comparative Analysis of France, Russia, and China*. Cambridge University Press.

Tucker, J. A., Theocharis, Y., Roberts, M. E., & Barberá, P. (2017). From liberation to turmoil: Social media and democracy. *Journal of Democracy*, *28*(4), 46–59.

United States: Freedom in the World 2021 Country Report. (2021). https://freedomhouse.org/country/united-states/freedom-world/2021

United States | Freedom House: Freedom on the Net. (2019). https://freedomhouse.org/country/united-states/freedom-net/2019

Waever, O. (1995). Securitization and Desecuritization. In R. D. Lipschutz (Ed.), *On Security*. Columbia University Press.

WGIG. (2005). *Report of the Working Group on Internet Governance* (Issue June). www.wgig.org

Whittaker, J. (2004). The Cyberspace Handbook. In *The Cyberspace Handbook*. Routledge.

Williams, M. C. (2015). Securitization as political theory: The politics of the extraordinary. *International Relations*, *29*(1), 114–120.

With Liberty to Monitor All. (2014).

Yashar, D. J. (2005). *Contesting Citizenship in Latin America: The Rise of Indigenous Movements and the Postliberal Challenge*. Cambridge University Press.