POLITICAL REGIME MATTERS?

FRAMING THE SPEECH ACT IN SECURITIZATION OF CYBERSPACE IN THE USA AND CHINA

By

Vlade Madžarević

Submitted to

Central European University

Department of International Relations

In partial fulfillment of the requirements for the degree of Master of Arts

Supervisor: Kristin Makszin

Word Count: 17.242

Budapest, Hungary

2016

Abstract

This thesis engages with the present academic debate in the field of security studies regarding the importance of context in securitization theory. More specifically, this discussion revolves around the problematic application of Copenhagen School's theory framework in non-democratic political contexts due to the theory's Western-centric bias, hence even questioning the possibility of securitization in such political settings. Through a configurative case study analysis of cyberspace securitization practices in the US and China, I empirically demonstrate that securitization indeed happens in both political regime contexts. In my research I apply systematic qualitative content analysis of the official documents and speeches concerning the US "Patriot Act" and the set of laws known as "The Great Firewall of China", and Vuori's five strands of securitization framework. The main findings of my research are that: 1) securitization does happen in both political regimes; 2) a long-term state of emergency can cause the democratic regimes to create a policymaking environment similar to that of the authoritarian regimes; 3) differences between the securitization procedure in the democratic and non-democratic political context does exist and it can be visible in how securitizing messages are framed and transmitted through the speech act to the target audience; 4) Vuori's framework based on the illocutionary logic for cross-contextual comparison of the securitization process requires additional strands to fully analyze the securitizing acts in the non-democratic political settings.

Acknowledgments

Dedicated to Lena, Vuk, and the rest of the “supporting crew”.

I would like to express my outmost gratitude to Prof. Kristin Makszin for providing me with all the ideas, guidance, patience, moral support, and infinite kindness throughout the process of thesis supervision.

Moreover, I would also like to thank Prof. Paul Roe for inspiring me to embark on a journey of exploring the topic of security studies.

Table of Contents

List of Tables

Introduction

The Internet, Cybersecurity, and Different Political Regimes

"We are all now connected by the Internet, like neurons in a giant brain".[1] These words by Stephen Hawking, truly one of the most brilliant minds in the entire human history, vividly describe the idea of how important cyberspace technology actually is as a source of information in the contemporary world. Reflecting on this extensive reliance on the internet and expanding on the metaphor used by Hawking, we can even argue that in a similar manner as the brain is crucial for cognitive understanding of the world and proper functioning of all the other organs in the human body that keep us alive, the internet is becoming, if not already, a vital element of our everyday life in terms of how we do things and perceive reality in general. According to Peter Warren Singer and Allan Friedman, although the cyberspace used to be only a realm of communication and e-commerce in the past, now it includes a wide range of areas labeled as the "critical infrastructure", which contain the "underlying sectors that run our modern-day civilization, ranging from agriculture and food distribution to banking, healthcare, transportation, water, and power".[2] Therefore, since so many important public sectors directly

Author's note: Certain parts of the presented research, and most notably sections entitled *Introduction* and *Chapter 1 – A Theoretical Framework for Understanding Securitization Across Contexts*, contain material that was previously developed by the author in several research papers submitted to the Department of International Relations of Central European University, Budapest, Hungary, during the 2015/2016 academic year. Moreover, the original and unedited documents containing the data regarding the qualitative content analysis of the two empirical cases examined in the research are available for inspection upon official request sent to the author on [*vlade.madzarevic@yahoo.com*].

[1] Jon Swartz, "Stephen Hawking Opens up," *Usatoday.com*, last modified December 1, 2014, http://www.usatoday.com/MONEY/usaedition/2014-12-02-QampA-with-Stephen-Hawking_ST_U.htm (accessed on 27.05.2016).

[2] Peter Warren Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, What Everyone Needs to Know (New York, USA: Oxford University Press, 2014), 15.

or indirectly depend on the internet, the priority of countries to protect their cyberspace became an issue of national security. Consequently, the doctrine of cybersecurity quickly emerged.

Cybersecurity is one of the most contemporary topics within the broader field of security studies. With rapid improvements in the IT sector and the mentioned tendency of shifting public and private services on the digital platform, cybersecurity is getting increased attention from both scholars and policy makers. The reason for this intensified focus is that while being an integral part of the everyday life of people, businesses, and institutions, the internet provides both opportunities and threats to its users. The example are social media websites, where individuals are providing a large amount of personal data on a voluntary basis. Now, this information can be used in providing better services to these individuals like targeted advertising or providing access to items of interest, but at the same time it can be abused like in cases of identity theft. Other dangers are numerous, from different types of malicious software and cybercriminals, to terrorists and cyberwarfare practices. Since any type of disturbance of cyberspace may cause a systematic disruption in the entire country, the main goal of cybersecurity is to identify and analyze these threats in order to provide strategies that will help governments, organizations, and individuals to protect important data, privacy, and critical infrastructure in the ever changing virtual environment. Yet, depending on the political context of the countries, the identified threats, motivations, and practices concerning the cyberspace security may differ significantly.

According to Ronald Deibert and Rafal Rohozinski, since the regime types and legitimacy differ greatly between the states, the actions taken in response to cyberspace risks vary correspondingly.[3] In other words, democracies will likely be reluctant to impose extreme measures without exceptional reason and strong public support, while authoritarian regimes

[3] Ronald J. Deibert and Rafal Rohozinski, "Risking Security: Policies and Paradoxes of Cyberspace Security," *International Political Sociology* 4, no. 1 (2010): 17.

will conversely have less boundaries in imposing measures such as censorship, surveillance, and control over internet due to the very nature of the political system in such cases. Although we can identify different types of non-democratic regimes, as pointed out by Juan Linz, for the simplicity reason I will use the term authoritarian regime in contrast to democracy throughout the paper.[4] Nonetheless, taking the above outlined stakes at hand, it is evident that both political contexts rank cyberspace high in their security agenda. Consequently, Deibert and Rohozinski claim that "[w]hether through cyberterrorism, or through accident, a growing recognition of all advanced societies' increasing dependence on cyberspace has brought about ever more pronounced efforts at cyberspace securitization".[5] In order to understand how this particular process of securitization takes place, we need to briefly examine the theoretical framework of the prominent concept and how it fits different political contexts.

Securitization in Democratic and Authoritarian Political Regimes

The securitization theory developed by the Copenhagen School of security studies represents a revolutionary turn in understanding the notion of security. The fundamental idea developed by Barry Buzan, Ole Waever, and Jaap de Wilde points out that any issue is not necessarily regarded as a security issue because it imposes a factual existential threat, but rather it is constructed and communicated as such.[6] The authors explain that "the exact *definition* and *criteria* of securitization is constituted by the intersubjective establishment of an existential threat with a saliency sufficient to have substantial political effects".[7] Put simply, a securitizing actor through the speech act communicates to the target audience that a referent object is under existential threat, and if the target audience accepts this message, the issue is securitized and

[4] Juan José Linz, *Totalitarian and Authoritarian Regimes* (London, UK: Lynne Rienner Publishers, 2000), 53–54.

[5] Deibert and Rohozinski, "Risking Security," 19.

[6] Barry Buzan, Ole Waever, and Jaap de Wilde, *Security : A New Framework for Analysis* (Boulder, Colorado: Lynne Rienner Publishers, 1998).

[7] Ibid., 25.

the securitizing actor has legitimacy to apply otherwise impermissible extreme measures in order to protect the referent object. However, the theoretical framework of Copenhagen School also left a fair share of vagueness in its argumentation, making it open to various ways of interpretation and hence very suitable for multiple lines of criticism.

One of the most important academic debates regarding the concept of securitization is on the topic of how important are the different contexts in which the theory is applied. The most prominent line of discussion is trying to clarify whether the Copenhagen School's theory can be universally applied in both democratic and non-democratic political regime settings, or it is primarily Western-centric and hence dependent on more liberal and transparent political practices. While in the democratic systems the concept of public accountability of the national governments and their political actions is something that is presumed even in the everyday state of affairs, and not to mention in some exceptional circumstances that require more extreme responses, the idea of public legitimacy for political decisions in the authoritarian regimes is generally perceived as something unnecessary due to the nature of the non-democratic rule. Nevertheless, according to Juha Vuori, purely coercive and repressive governance is unsustainable in the long run and it can easily backfire to the oppressor, thus even the authoritarian regimes need to legitimize their actions, and the idea of security always serves as a good justification in these political settings.[8] On top of that, Johannes Gerschewski suggests that along with repression and co-optation, legitimation represents one of the three pillars of stability of the autocratic regimes.[9]

[8] Juha A. Vuori, "Illocutionary Logic and Strands of Securitization: Applying the Theory of Securitization to the Study of Non-Democratic Political Orders," *European Journal of International Relations* 14, no. 1 (March 1, 2008): 68.

[9] Johannes Gerschewski, "The Three Pillars of Stability: Legitimation, Repression, and Co-Optation in Autocratic Regimes," *Democratization* 20, no. 1 (January 1, 2013): 14.

The academic debate on the topic, which I will reflect on in more detail in the following chapter of my analysis, reveals at least three gaps in the literature that remain to be explored. First of all, the critics of the theory do not openly neglect the fact that securitization is actually happening in the authoritarian regimes, however it is unclear whether the points they emphasize as flaws in the original concept are systemic in nature or they just represent exceptional circumstances that could be incorporated into the current framework. In other words, the question whether the non-democratic regimes set entirely new rules for securitization on a universal and consistent basis, or they just interpret the existing guidelines in a different way, still remains unanswered. Secondly, due to the lacking number of cases where the securitizing acts are directly compared across the diverging contexts, it seems that assumptions about the securitization in democratic political regime settings are often taken for granted by the critics. Hence, in order to draw any meaningful conclusion on the debated topic, there is a need for direct comparison of cases examining the securitization practices in both democratic and non-democratic settings. Lastly, except Juha Vuori, the debate regarding the speech act mostly focuses on the conceptual appropriateness of the act within the process of securitization, rather than on its essence – the message to the target audience. Since the speech act is identified as a crucial segment of the Copenhagen School's framework, examining the exact language used in the process of message framing can be vital for cross-contextual comparison.

Therefore, the main aim of my research is the following: can we identify dissimilar patterns of framing the securitizing messages to the target audience between the securitizing actors of different political regime types? If yes, how does the rhetoric applied in the process of securitization deviate between democracies and non-democracies? If no, how can we explain this counterintuitive phenomenon, and to what extent does the context in that case play a significant role in the securitization process? Moreover, since the democratic and authoritarian political regimes exhibit considerable differences in a variety of aspects, the intuitive hypothesis is that there should be dissimilarity in the way how these two political systems frame their messages to the target audience in the process of securitization. One unique aspect of my research is that I will analyze the securitization process in a democratic and a non-democratic context side-by-side. This will enable greater understanding of how securitization 'travels' to a new context and what, if any, parts of it need to be adapted for its application in a non-democratic context.

Methodological Approach

In my analysis, I will apply configurative case study comparison approach of cyber securitization practices in the USA and China. This method of investigation will allow me to compare the prospective dissimilarities or resemblances of the securitization process across the diverging contexts, allowing me to potentially find certain characteristic patterns of the securitizing message framing for the examined settings. The reason I am taking these two particular countries in my analysis is the fact that they are both equally important actors in the realm of global geopolitics, but evidently on completely different ends of the spectrum in terms of the political regime type. Since it is very hard to find relevant and comparable cases between these two diverse backgrounds, I have decided to examine the practices of securitization in cyberspace as the most ideal context to conduct my research.

Considering that cyberspace is a single public domain without any existing parallel constructions, it represents a common ground that offers equal opportunities and threats to each actor participating in its boundaries, regardless of the background these actors come from. Moreover, my analysis will build on the contemporary concept of cyber securitization that was introduced by Lene Hansen and Helen Nissenbaum. According to them, cybersecurity is a distinct sector with a particular constellation of threats and referent objects within the original theoretical framework of the Copenhagen School, which is tightly connected to the collective referent objects of the four other sectors - “the state,” “society,” “the nation,” and “the economy”.[10] Hence, from the perspective of modern security studies, we can see that cyber securitization is equally important as any other type of securitization practice. Moreover, since both hardware and software required for utilization of different aspects of the cyberspace are essentially the same for everyone, correspondingly all the capabilities, practices, and tools provided by the digital platform are fundamentally the same and equally at disposal for anyone. Hence, along with the common tools used in the process, the decisions and actions taken by the governments in pursuit of enhancing the cybersecurity are more universal for different political contexts than it is the case with most other policy areas.

Regarding the securitization framework, I fix the securitizing actor in terms of a state/government (USA and China), while the target audience will be solely viewed in terms of an overall population of the two countries. Furthermore, the emphasis is put on a speech act made by the securitizing actor only, regardless of the specific type of referent object taken into consideration. In this way I ensure the comparability of the securitizing acts made by the opposing regimes, and at the same time narrow down the scope of the literature that I review in the research process. Consequently, I isolate the conditions that will allow me to examine the effects of diverging regimes on the way how the messages to the target audience are framed in the process of securitization. In my interpretation of the speech acts transmitted by the securitizing actors, I will use the framing analysis approach in combination with the “Five Strands of Securitization” framework developed by Vuori.

The empirical cases of regulation of cyberspace that I will observe are revolving around the US “Patriot Act” introduced after the 9/11 terrorist attacks, and the Chinese extensive internet regulation widely known as “The Great Firewall of China”. More precisely, I will focus

[10] Lene Hansen and Helen Nissenbaum, “Digital Disaster, Cyber Security, and the Copenhagen School,” *International Studies Quarterly* 53, no. 4 (December 1, 2009): 1155.

on the state justification of the “Enhanced Electronic Surveillance Procedures” granted by the “Patriot Act” in the US case, and justification for a set of strict internet regulations provided by the government’s “White Paper” in Chinese case. The mentioned empirical cases are potential instances of cyberspace securitization in two countries that represent the most prominent cases of the differing political regime types. Moreover, in my analysis I will use both primary and secondary sources. In the US case I will examine the official legislative documents and the supporting specialized committee reports, the official statements made by the President and the members of the US Congress, and the reports provided by the Department of Justice regarding the proposed/passed bills, all in the 2001-2006 period, ending with the first extension of the sunset clause. In the Chinese case I will observe the official legislative documents from 1994-1997, along with the specialized and comprehensive “The Internet in China” report officially published in 2010 by the Chinese government. Since my attention is on the primary justifications for surveillance and restrictions, these particular sources are best suited for my intended analysis. Similarly, the secondary sources will deal with the mentioned cases from an academic perspective, and some of them will examine the regime type differences, and the engagement of the mentioned countries in the field of cybersecurity.

Relying on the above mentioned documents, I have conducted a qualitative content analysis in which I systematically asked the following set of questions related to each text: Who prepared the document? What is the purpose of a document? Whom it was targeted to? What is the core justification? Who/What is the threat? Who/What is threatened? Based on the outlined questions, I initially investigated whether both cases were indeed instances of securitization. I have done this by thoroughly identifying and marking the specific words present in the examined texts that designated the core elements of the practice of securitization. In the next stage of analysis, I have analyzed the words and phrases used as a part of justification for the securitizing act. Here I mostly concentrated on the nature of the message and the number of times these specific sets of words/phrases were used in the text, after which I would classify them in separate thematic categories. After the classification phase for each of the examined text, along with the other elements of securitization, I have compared these broad justifying speech act categories within the same political context, aiming to identify trends, the message framing patterns, and any potential changes over time regarding the overall securitization procedure. Finally, in the last phase of qualitative content analysis, I have compared the results across the differing political contexts in order to gain some general insights regarding the similarities and differences of the securitization process in democratic and non-democratic regimes.

Contribution of the Research

Using this approach, my thesis makes a core contribution to the literature in the following ways. First of all, it takes on the challenge of comparative analysis of the process of securitization in two differing regime types within a single project. Even Vuori who developed the framework that could be applied in both political contexts did not conduct a direct comparison of securitizing acts between the democracies and non-democracies. My research contributes to the existing academic debate regarding the contextualization of securitization by empirically demonstrating that securitization process does occur in both political regimes. However, I also contribute to this debate by revealing concrete differences between the securitization practices in democratic and authoritarian contexts, and claim that this dissimilarity is mostly visible in how these political regimes frame and disseminate the securitizing message to the target audience. Furthermore, since Vuori’s framework has rarely been applied outside of the non-democratic empirical context that was used to develop it, my research contributes to the literature by testing the “five strands of securitization” concept in both political settings. Moreover, my research improves Vuori’s theoretical framework by identifying the additional strands of securitization that are overlooked by the original concept.

Research Structure

In Chapter 1 of my research, I will briefly revisit the existing academic debate on the topic of contextualization of securitization, focusing mainly on the impact of political regimes on the securitization process and questions regarding the universal application of the Copenhagen School's theory across contexts. In the remaining part of the chapter, I will outline the main conceptual guidelines of Vuori's five strands of securitization framework that I will later apply in the empirical analysis, and I will also briefly summarize the main claims of my research deriving from the literature and empirics. In Chapter 2, I will examine the empirical cases of cyber securitization in the US and China. In this section I will mainly focus on the analysis of legislative acts that prescribed the enhanced measures in an attempt to securitize different issues regarding cyberspace in both contexts. In this section I will also reflect on the implications of these measures that can be understood as "above politics". In Chapter 3, I will apply Vuori's five strands framework in a comprehensive empirical analysis of the cyber securitization practices in the two outlined cases with differing political regimes. In the last part of the same chapter, I will systematically present the main findings of the conducted research. Finally, in the concluding chapter I will briefly revisit the main points and contribution of the examined study, with a short reflection on the research limitations and possibilities for further analysis on the topic.

Chapter 1 – A Theoretical Framework for Understanding Securitization Across Contexts

In this section I will briefly examine the existing literature and the ongoing academic debate on the topic of whether the Copenhagen School's theoretical framework is applicable outside of the Western liberal-democratic context. I will mainly focus on the literature speaking about the contextual differences between the democratic and non-democratic regimes, and how the original securitization theory fits these two dissimilar political backgrounds. My goal here is to explore the conceptual basis of the Copenhagen School's theory that allows universal application of its framework across the different political environments. Moreover, I will also present the concept developed by Juha Vuori who highlighted the importance of understanding the full complexity of the speech acts used in the securitization procedure. The five strands of securitization framework developed by Vuori has an aim to provide a universal mechanism for "conceptual travel" of Copenhagen School's theory without "conceptual stretching".[11] Finally, in the last subsection of this chapter, I will briefly summarize the main theoretical contribution of my research deriving from the examined academic literature and the conducted empirical analysis.

1.1 Contextualization of Securitization

The academic debate regarding the securitization theory and its universal applicability across different political contexts starts with the criticism that the Copenhagen School's framework is exceedingly Western-centric, and thus conceptually locked in what is widely identified as the "Westphalian straitjacket". The idea of "Westphalian straitjacket" was developed by Barry Buzan and Richard Little, and it denoted a strong ahistorical tendency of

[11] Vuori, "Illocutionary Logic and Strands of Securitization," 66.

the International Relations (IR) to persistently understand the global geopolitical system, regardless of time and space, through the lenses of the model established in seventeenth century Europe.[12] Put differently, if the theoretical framework is applied in contexts that differ significantly from the core Western liberal-democratic values and practices, it will face variety of conceptual problems and virtually be inapplicable in these political settings. According to Claire Wilkinson, this is exactly what happens with the Copenhagen School's theory. Wilkinson points out that due to the theory's overreliance on the Western-centric contextual assumptions, the exclusive emphasis on the verbal type of communication in the process of securitization is conceptually problematic, which becomes evident when the theory is applied in non-democratic political contexts where the majority of population is usually unable to freely express their political and societal concerns.[13]

Furthermore, while agreeing with Wilkinson's argument and highlighting the new ways and platforms of communication due to the technological developments, Michael Williams points out that "presentation of security as a speech-act is potentially too narrow to grasp fully the social contexts and complex communicative and institutional processes of securitization at work in contemporary politics".[14] Yet, it is not conceptually clear how could non-verbal deeds be intersubjectively interpreted as the obvious securitizing attempts on their own, meaning that we still need speech acts to interpret them in such a way. On the other hand, Thierry Balzacq challenges the idea of the Copenhagen School regarding the central role of the speech act in defining the security issues. Besides containing a well-structured speech act, Balzacq suggests that an effective securitization is highly context dependent, audience-centered, and power-

[12] Barry Buzan and Richard Little, "Why International Relations Has Failed as an Intellectual Project and What to Do About It," *The Millenium Journal of International Studies* 30, no. 1 (2001): 24–26.
[13] Claire Wilkinson, "The Copenhagen School on Tour in Kyrgyzstan: Is Securitization Theory Useable Outside Europe?," *Security Dialogue* 38, no. 1 (March 1, 2007): 7–8, 12–13.
[14] Michael C. Williams, "Words, Images, Enemies: Securitization and International Politics," *International Studies Quarterly*, 2003, 528.

laden.[15] This implies that specific circumstances provided by the contextual background (e.g., the regime type) will considerably influence both the level of authority or power that securitizing actor has, and the readiness of the target audience to accept the securitizing message.

Monika Barthwal-Datta builds on this critique and points out that the emphasized importance of the speech act in the securitization framework is ultimately favoring the state as the socially and politically most powerful player in the role of securitizing actor, while at the same time neglecting all the other important participants who do not have access to traditional sources of power, but possess the knowledge, capabilities, or experience to identify threats.[16] Following this argument, Lene Hansen outlines the idea of "security as silence", which occurs in contexts when "insecurity cannot be voiced, when raising something as a security problem is impossible or might even aggravate the threat being faced".[17] Deriving from the arguments of Barthwal-Datta and Hansen, there is a possibility that the authoritarian states and overly repressive political regimes might be perceived by their society as the main threat to the national survival, which creates a peculiar situation of having two competing securitizing attempts within one context, the one from the leadership to preserve its security and authority, and the one from society wanting to remove this authoritarian regime.

On the other hand, the notion of competing securitizing acts is not completely unfamiliar in the existing academic debate. The discussion about it can be found in the respective research of Nicole Jackson and Stefan Elbe. Jackson presents the concept of "security dichotomies", which in essence explains the situation when a certain security issue

[15] Thierry Balzacq, "The Three Faces of Securitization: Political Agency, Audience and Context," *European Journal of International Relations* 11, no. 2 (June 1, 2005): 179, 192.
[16] Monika Barthwal-Datta, "Securitising Threats without the State: A Case Study of Misgovernance as a Security Threat in Bangladesh," *Review of International Studies* 35, no. 2 (2009): 300.
[17] Lene Hansen, "The Little Mermaid's Silent Security Dilemma and the Absence of Gender in the Copenhagen School," *Millennium - Journal of International Studies* 29, no. 2 (June 1, 2000): 287.

has two contradictory understandings, out of which one is positive and the other one is negative.[18] By encountering the outlined situation while exploring the topic of HIV/AIDS securitization, Elbe argues that such securitizing act can at the same time enhance the awareness and funding of the international AIDS initiatives, but it can also backfire and directly endanger civil liberties of the people living with HIV/AIDS under certain circumstances.[19] Following the logic presented by the two authors, if an individual actor may perceive a particular security issue in two different ways, logically the two different actors might perceive the same security issue in a contrasting manner as well. Accordingly, in the context of securitization theory, the rational assumption is that if the securitizing actors are originating from different backgrounds, like in the case of different political regime types, they will probably have different perceptions of whether certain security issues should be essentially securitized or not.

Nevertheless, probably the biggest conceptual challenge for the universal application of securitization across different political contexts is the concept of "normal politics". According to Copenhagen School, the securitization criteria is ultimately fulfilled only when existential threats legitimize the breaking of rules, meaning that actions undertaken shift from the realm of normal politics to the realm beyond politics.[20] Jackson doubts the notion of "normal politics" in authoritarian regimes as the majority of the decisions are done in "emergency mode" with little or no public legitimization.[21] Put simply, since the authoritarian regimes in general do not need to legitimize their actions to the audience, then securitization has limited (if any) applicability in such political contexts. On the other hand, Juha Vuori points

[18] Nicole J. Jackson, "International Organizations, Security Dichotomies and the Trafficking of Persons and Narcotics in Post-Soviet Central Asia: A Critique of the Securitization Framework," *Security Dialogue* 37, no. 3 (September 1, 2006): 308–309.
[19] Stefan Elbe, "Should HIV/AIDS Be Securitized? The Ethical Dilemmas of Linking HIV/AIDS and Security," *International Studies Quarterly* 50, no. 1 (2006): 120.
[20] Buzan, Waever, and de Wilde, *Security : A New Framework for Analysis*, 23–25.
[21] Jackson, "International Organizations, Security Dichotomies and the Trafficking of Persons and Narcotics in Post-Soviet Central Asia," 311–312.

out that purely oppressive rule is unsustainable in the long run, thus "even the most despotic states are headed by individuals who depend on the favorable beliefs of some key figures in the polity".[22] In other words, although the securitization in authoritarian contexts might not be done in the same way or even with the same motivation and purpose like in the democratic political systems, this does not mean that it is nonexistent or unnecessary in such settings.

Although strongly criticizing the original framework on several grounds, neither one of the examined critics is openly rejecting the possibility of securitization occurring in different political contexts. Yet, if applied in disparate political settings, the Copenhagen School's flagship theory is undoubtedly demonstrating a considerable amount of conceptual inconsistencies. Thus, if we would like to conduct a cross-contextual comparison of securitization practices, due to the very nature of different regimes and their types of political governance, we would face huge problems to find two completely identical (i.e., comparable) cases. Considering the core elements of securitization, on the first look only securitizing actors and the audience remain with more or less limited deviations. As already stated, the perception of actors regarding the security issues (threats and referent objects) can vary substantially even within the same political system. However, since the core idea of the Copenhagen School's framework is that security is constructed as such by the actors, the specific choice of threats and referent objects does not matter too much from the theoretical perspective, as their overall conceptual meaning will always remain the same. Similarly, although it may differ, the speech act is equally utilized by both democratic and non-democratic regimes for the same purpose on a consistent basis. Noticing this, Vuori started developing the framework based on the common speech act logic in order to provide a universal tool for securitization analysis across different regime contexts.

[22] Vuori, "Illocutionary Logic and Strands of Securitization," 68.

1.2 Vuori's Five Strands of Securitization

Following the basic principle of the Copenhagen School's theory, Vuori points out that "[i]f security issues are constituted through a process of speech acts, they should be constituted through the same mechanism in all societies".[23] As mentioned earlier, it is suggested here that the speech act has the same role to transmit the securitizing message within any context, regardless of the content and even language spoken. Thus, Vuori's key assumption is that the "explication of the act of securitization is based on illocutionary logic".[24] According to John Searle and Daniel Vanderveken, there are five basic illocutionary points: 1) assertive (say how the things are); 2) commissive (commit the speaker to doing something); 3) directive (try to get other people to do things); 4) declarative (change the world by saying so); and 5) expressive illocutionary force (express feelings and attitudes).[25] Put simply, the theory suggests that even the most complex speech constructions are based on these five basic categories. Since the mentioned illocutionary points differ in their nature, logically the speech acts based on each of these categories will deviate in a similar manner. Building on the presented logic and by empirically analyzing the speech acts commonly used in the processes of securitization, Vuori identified five different strands of securitization (see Table 1), which considerably expanded the original Copenhagen School's framework regarding the speech act construction.[26]

As briefly summarized in Table 1, these five strands of securitization are the following: 1) rising an issue to agenda; 2) legitimizing future acts; 3) securitization for deterrence; 4) legitimizing past acts / reproducing security issues; 5) securitization for control. Evidently, the proposed classification is suggesting that securitization can be applied for a range of political actions, and not only for legitimization of future acts as implied by the original Copenhagen

[23] Ibid., 73.
[24] Ibid., 66.
[25] John Searle and Daniel Vanderveken, *Foundations of Illocutionary Logic* (Cambridge, UK: Cambridge University Press, 1985), 37–38.
[26] Vuori, "Illocutionary Logic and Strands of Securitization," 75–76.

School's theory. In that light, Vuori, suggests that "the complex act of securitization can contain several kinds of perlocutionary intentions and effects, and thus, that securitization can be utilized for a range of political purposes".[27] Therefore, by focusing on the language as an essence of the securitizing speech act that transcends both time and space, Vuori developed the framework that can be equally applied in different political contexts for a purpose of identifying similarities and differences in securitization practices between diverse political settings.

Table 1 - Vuori's Five Strands of Securitization

Strand of Securitization	Elementary Speech Act	Illocutionary Point	Perlocutionary Aim	Temporality	Debate
Rising an Issue	Claim, Warn, *Suggest*	Directive	Convincing	Future	Yes
Legitimizing Future Acts	Claim, Warn, *Request*	Directive	Legitimacy	Future	Yes
Deterrence	Claim, Warn, *Declare*	Declarative	Deterrence / Intimidation	Future	No
Legitimizing Past Acts / Reproducing Security	Claim, Warn, *Explain*	Assertive	Legitimacy	Past	Yes
Control	Claim, Warn, *Require*	Directive	Obedience / Discipline	Future	No

However, as Table 1 also demonstrates, each strand contains certain characteristics that are clearly diversifying it from the other four strands, and imposing basic criteria based on which speech acts should be identified and categorized. First of all, from the second column in Table 1, we can see that Vuori understands the securitizing speech act as a complex and

[27] Ibid., 66.

sequential construction. Evidently, each category starts with a claim that explains the general state of affairs regarding some issue at present or in the past (depending on temporality – the fifth column in Table 1), and it is followed by a warning that explains why this issue needs/had to be tackled by someone. This sequence is further continued by the third (varying) string that, by containing the appropriate illocutionary point and perlocutionary aim, ultimately reveals which goal the securitizing actor has by communicating the message. Now, as Searle and Vanderveken point out, different illocutionary points have differing conditions to be achieved.[28] Hence, if the securitizing actor is "requesting" something to be done, this can only mean that such speech act is "directive", since directives include speech acts such as requests, commands, advices, etc. The same thing is true with other types of communication.

Therefore, by using this logic proposed by Searle and Vanderveken and analyzing the empirical cases of securitization in both political contexts, Vuori set the list of five different strands of securitization that exist in practice and have their own unique elements that construct them. As already mentioned, the main goal of Vuori's framework was to enable application of securitization analysis in, as we could see from the literature, conceptually problematic non-democratic context. Put differently, by offering universally applicable analytical guidelines based on language, the proposed theoretical structure was ambitiously aiming to finally move securitization from widely perceived "Westphalian straitjacket" bias. Thus, according to Vuori, if we want to precisely understand who can securitize, which threats, for whom, why, with what effects, and under which conditions, then we ought to investigate the securitizing speech acts in as many contexts as possible.[29] Since there are hardly any similar approaches in the existing literature on the Copenhagen School's theory as Vuori's one, the five strands of

[28] Searle and Vanderveken, *Foundations of Illocutionary Logic*, 38–40.
[29] Vuori, "Illocutionary Logic and Strands of Securitization," 68.

securitization framework represents one of the key tools currently available for the cross-contextual comparison of the securitization process in different political regimes.

1.3 The Argument

Informed by the empirical research presented in the following two chapters, I have four major claims to make. First of all, responding to the existing academic debate on the topic, I claim that securitization can happen in both political regime contexts. Secondly, I claim that the democratic regimes under the long-term state of emergency, over time develop similar policymaking climate as their non-democratic counterparts. Thirdly, I claim that the process of securitization in democracies differs from the one happening in the authoritarian regimes in the way how securitizing actors frame the messages disseminated through the speech act to the target audience. Lastly, I claim that Vuori's five strands of securitization framework is insufficient to fully realize the process of securitization in the non-democratic political regime contexts, due to fact that it is overlooking several possible securitization strand constructions that are empirically identifiable in the mentioned political settings. Therefore, in order to verify my presented claims, in the next two chapters I will conduct an empirical analysis of the regulation of cyberspace in both democratic and non-democratic political regime context.

Chapter 2 – The “Above Politics” Measures and Different Regimes

According to the Copenhagen School’s framework, the securitization criteria is not satisfied solely by breaking the rules or only by existential threats, but rather these standards are fulfilled when we have cases of existential threats that legitimize the use of extreme measures that break the rules.[30] For that reason, although the concept of cyber security and the corresponding scientific discourse were rapidly developing since the early 1990s, Hansen and Nissenbaum point out that for a long time the idea of cyber security was considered as an “attempted securitization” by the Copenhagen School.[31] Yet, with the continuous development of information technology, the new types of threats also emerged. The hackers, cybercriminals, cyberterrorists, along with different types of spyware, malware, and cyber fraud practices, significantly influenced both researchers and national governments to seriously consider these emerging dangers as contemporary security issues. However, since the concept of cyber securitization is relatively new within the broader field of security studies, it is still debatable whether it can be understood as an independent securitization practice. In this chapter, by examining two separate cases, I will empirically demonstrate that not only the practice of cyber securitization does exist, but that it also exists in both democratic and non-democratic contexts.

2.1 The Origins of Enhanced Electronic Surveillance Measures in the US

The terrorist attack on the 11th of September 2001 (9/11) is commonly regarded as the most serious attack on the US soil after the World War II and the Pearl Harbor bombing. The 9/11 events introduced a completely new type of threat in the shape of the transnational terrorist groups, organized and coordinated with the help of the modern information technologies, and

[30] Buzan, Waever, and de Wilde, *Security : A New Framework for Analysis*, 25.
[31] Hansen and Nissenbaum, “Digital Disaster, Cyber Security, and the Copenhagen School,” 1155–1156.

ready to strike decisively and unnoticed on any place of the Earth. Moreover, this terrorist act revealed the numerous vulnerabilities and obsolete practices in the US systems of defense, intelligence, federal legislation, law enforcement, and the national security in general. Consequently, on the 14th of September 2001, a state of "national emergency" was proclaimed by the President George W. Bush due to the "continuing and immediate threat of further attacks on the United States".[32] While the country was still mourning over the innocent victims, the American society expected a strong response from the President Bush Administration. The answer quickly came in a form of the USA PATRIOT Act (the Patriot Act). On the 23rd of October 2001, only one month after the terrorist attacks, the legislation entitled "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001" was introduced by the Congressman James Sensenbrenner, and after passing the House of Representatives and the Senate, it was signed into law by the President Bush on the 26th of October.[33]

From the securitization theory perspective, although the imposed state of emergency itself represents the extreme measure that qualifies as "above politics", the Patriot Act touches and outlines the specific areas that need to be secured, and one of them is cyberspace. These enhanced measures that are both directly or indirectly concerning cyberspace are mainly defined in the most controversial section of the Patriot Act under the Title II named as the "Enhanced Surveillance Procedures" (Appendix 1). Moreover, further bills and official strategies concerning the US cyberspace were introduced in the following years, such as the "Cyber Security Enhancement Act of 2002" and "Homeland Security Act of 2002",

[32] Gerhard Peters and John T. Woolley, "George W. Bush: Proclamation 7463 - Declaration of National Emergency by Reason of Certain Terrorist Attacks," *The American Presidency Project*, last modified September 14, 2001, http://www.presidency.ucsb.edu/ws/?pid=61760 (accessed on 26.04.2016).

[33] Library of Congress, "Summary of H.R.3162 - 107th Congress (2001-2002): Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001," *Congress.gov*, last modified October 26, 2001, https://www.congress.gov/bill/107th-congress/house-bill/3162/summary/81 (accessed on 23.04.2016).

accompanied by "The National Strategy to Secure Cyberspace" from 2003. These items had a goal to either fill-in the gaps of the Patriot Act provisions, or to even further expand the competencies granted by this controversial law. Exactly for this reason, in order to emphasize that such debatable provisions will only exist temporarily for the imminent threat repealing purposes, the "Sunset" clause (Sec. 224) of the Patriot Act guaranteed that most of the articles under the Title II will cease to exist on the 31st of December 2005.[34] For the purpose of understanding why such a move was necessary in the democratic regime context, we need to briefly examine these enhanced measures.

Although the titles of sections 201-202 regarding the interception of different types of communication are self-explanatory, it is important to note that the phrase "electronic communication" refers to "the transfer of information, data, or sounds from one location to another over a device designed for electronic transmissions".[35] Under the appropriate suspicion, from the cyber securitization point of view this meant that the private emails and any other type of electronic exchange of data with the internet could become a subject of governmental surveillance. Accordingly, the section 203 permits the intercepted information gained through the "foreign intelligence or counterintelligence" practices to be shared between the different Federal agencies and officials, while the section 206 allows the roving surveillance authority in the situations "where the Court finds that the actions of the surveillance target may have the effect of thwarting the identification of a specified person".[36] This essentially empowered the authorities to unimpededly surveil and share the collected data from the multiple electronic devices in any way connected to the targeted suspect. On top of that, the

[34] James Sensenbrenner, *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001*, 2001, sec. Title II-Enhanced Surveillance Procedures (Sec. 201-225), 295, https://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf (accessed on 23.04.2016).

[35] Legal Information Institute, "Electronic Surveillance," *Cornell.edu*, last modified July 17, 2008, https://www.law.cornell.edu/wex/electronic_surveillance (accessed on 03.05.2016).

[36] Library of Congress, "Summary of H.R.3162 - 107th Congress (2001-2002)."

Patriot Act increased the number of district judges designated to approve the mentioned forms of electronic surveillance from seven to eleven, as it is outlined under the section 208.[37] In this way, the issuing of wiretapping warrants became a much quicker and more efficient process.

Furthermore, sections 213 and 219 regarding the issuing of warrants enabled "a delay of required notices of the execution of a warrant if immediate notice may have an adverse result and under other specified circumstances" and permitted the "Federal magistrate judges in any district in which terrorism-related activities may have occurred to issue search warrants for searches within or outside the district," respectfully.[38] Put differently, the advanced electronic surveillance of the suspects could be utilized by the government agencies for the unspecified period of time without official notice, virtually on the territory of the entire country. The scope of enhanced electronic surveillance competencies authorized by the law became even wider with sections 214 and 215. The first allowed the use of pen register devices (including the electronic devices) in obtaining the "foreign intelligence information" (i.e., the surveillance purposes), while the second licensed the high ranking Federal officials to access various types of tangible things (including the digital records) in "investigation to protect against international terrorism or clandestine intelligence activities".[39] Finally, section 225 guarantees the legal immunity to a "provider of a wire or electronic communication service, landlord, custodian, or any other person that furnishes any information, facilities, or technical assistance," requested by the appropriate legal body.[40] From the perspective of a country with such strong democratic tradition, the presented provisions do appear exceptional in many ways.

[37] Sensenbrenner, *USA Patriot Act of 2001*, sec. Title II-Enhanced Surveillance Procedures (Sec. 201-225), 283.
[38] Library of Congress, "Summary of H.R.3162 - 107th Congress (2001-2002)."
[39] Sensenbrenner, *USA Patriot Act of 2001*, sec. Title II-Enhanced Surveillance Procedures (Sec. 201-225), 286-287.
[40] Library of Congress, "Summary of H.R.3162 - 107th Congress (2001-2002)."

2.2 The Origins of "Great Firewall of China"

On the other hand, the enhanced cyberspace intervention in China dates as early as the 1990's. The first set of regulations were already introduced in 1994, followed by comprehensive "Computer Information Network and Internet Security, Protection and Management Regulations" from 1997, which imposed a wide set of restrictions to the public and granted the full control of Chinese cyberspace to the authorities. The policy direction of the Chinese government seems to be a reaction to several events that occurred in the 1989-1995 period, most notably the student-led Tiananmen Square protests in Beijing, as well as the fall of the Iron Curtain and communist regimes in Central and Eastern Europe.[41] Clearly, the Chinese Communist Party (CCP) leadership needed to take a set of decisive actions to preserve stability within the country in order to avoid the fate of the mentioned falling regimes. In that light, learning from the experience of the Tiananmen Square dissent that has been considerably fueled by dissemination of the views contrasting the government ones through portable radios (i.e., use of technology), the Chinese government started developing "the most sophisticated Internet filtering system in the world".[42] Considering these facts, it becomes obvious that some of the main motives behind the heavy regulation of cyberspace in China are preservation of CCP regime and social stability.

These motivations were either explicitly or implicitly expressed in the legislative acts themselves. In the 1994 act labeled "Regulations for Safety Protection of Computer Information Systems", the Article 1 states that the purpose of this law beside the labeled safety is to "promote the application and development of computers and safeguard the smooth

[41] Jeffrey N. Wasserstrom, *China in the 21st Century: What Everyone Needs to Know*, What Everyone Needs to Know (New York, USA: Oxford University Press, 2010), 76–78.

[42] Hall Gardner, "War and the Media Paradox," in *Cyber Conflict and Global Politics*, ed. Athina Karatzogianni, Contemporary Security Studies (Taylor & Francis, 2008), 20.

fulfillment of socialist modernizations".[43] The emphasis here is clearly on the term "socialist modernization" which has a goal to distinguish such practice from any other in the world, while at the same time being vague enough to be understood in political, social, ideological, and economic sense. Correspondingly, the aim of previously mentioned regulation from 1997 was to "strengthen the security and the protection of computer information networks and of the Internet, and to preserve the social order and social stability".[44] Evidently, the social order and stability is inseparably linked to the concept of cyberspace security according to the Chinese government. Put differently, the internet became something more than just a mere technological advancement, but it was also understood as a fertile ground and potential source of some existential threats to the country (i.e., regime). Hence, from the perspective of the CCP, the extensive securitization of cyberspace was a necessary and logical strategy aiming to safeguard the regime and social order in the country.

These enhanced measures that could be classified under the Copenhagen School framework as above politics are situated in the provisions of the observed regulations from 1994 and 1997. Under Article 7 of the former it is stated that "[a]ny organization or individual shall not make use of computer information systems to engage in activities harmful to the interests of the state, collectives and citizens", while Article 17 authorized public security agencies to supervise and instruct, to investigate and handle crime, and "perform other supervisory responsibility for the safety protection work of computer information systems".[45] In other words, the cyber activities that are perceived as harmful for the state and society are

[43] Asian Legal Information Institute, tran., "Regulations of the People's Republic of China for Safety Protection of Computer Information Systems," *Asianlii.org*, http://www.asianlii.org/cn/legis/cen/laws/rfspocis719/ (accessed on 07.04.2016).

[44] Lehman, Lee & Xu, tran., "Computer Information Network and Internet Security, Protection and Management Regulations," *Lehmanlaw.com*, http://www.lehmanlaw.com/resource-centre/laws-and-regulations/information-technology/computer-information-network-and-internet-security-protection-and-management-regulations-1997.html (accessed on 07.04.2016).

[45] Asian Legal Information Institute, "Regulations of the People's Republic of China for Safety Protection of Computer Information Systems."

not clearly defined in order to leave the space for a wider interpretation, while the legal right to actively surveil, direct, and sanction such cyberspace activities was granted to the government. Likewise, the 1997 act under Article 4 points out that no entity "may use the Internet to harm national security, disclose state secrets, harm the interests of the State, of society or of a group, the legal rights of citizens, or to take part in criminal activities".[46] By introducing this provision, the Chinese government for the first time explicitly identified the concept of internet security as a genuine part of the overall national security.

Furthermore, the internet was officially put under governmental control with the regulation from 1997 which prescribed under Article 6 (1) that no entity "may use computer networks or network resources without getting proper prior approval" by the designated authorities, while Article 8 firmly stated that all entities involved in "Internet business" (i.e. licensed internet providers) must accept "the security supervision, inspection, and guidance of the Public Security organization", including delivery of digital information and materials that might help in discovering criminal activities.[47] However, the most controversial provision was Article 5 which literally had a goal to censor the cyberspace content within the country. This section prohibited entities to "create, replicate, retrieve, or transmit" the information that incites actions: to resist or break the Constitution or laws; to overthrow the government or the socialist system; division of the country; hatred or discrimination among nationalities; spreading rumors that are destroying the order of society; promoting different type of vices and violence; terrorism or other criminal activities; and injuring the reputation of state organs.[48] Similarly to the US case, these two legislative acts from 1994 and 1997 created a foundation for the future laws that had a goal to cover almost every part of the Chinese cyberspace (Appendix 2).

[46] Lehman, Lee & Xu, "Computer Information Network and Internet Security, Protection and Management Regulations."
[47] Ibid.
[48] Ibid.

2.3 Implications of the Enhanced Measures

Under the excuse of exceptional circumstances, the US Administration relatively easily managed to persuade the public that the enhanced measures provided under the Patriot Act are solely for the purpose of fighting the threat of terrorism. As we could see, the legitimacy of the decision was further enforced by the "Sunset" clause which promised the expiry date for these exceptional measures for a reasonable amount of time until the imminent threat is deterred. Yet, this has not happened. The sections set to expire under the "Sunset" clause were extended in 2006 with the "USA PATRIOT Improvement and Reauthorization Act".[49] In the future, the provisions of the bill were extended for several times with minor changes, while the last one happened in a form of the "USA Freedom Act" signed by President Barack Obama in 2015, which is in force at present.[50] Hence, the enhanced measures that were justified and accepted by the citizens as exceptional and temporary, almost unnoticeably continued their lifespan for more than a decade.

According to Jef Huysmans who also examined the post-9/11 events, the very core of the problem is what he labels as "political exceptionalism" that twists the traditional liberal-democratic matrix of political power, which ultimately leads to gradual undermining of the restraining effects of the rule of law on political discretion, and distortion of the liberal-democratic technique of representing popular will in political leadership.[51] In other words, when democracies start to implement the practices of political exceptionalism, such as enacting the controversial provisions under the Patriot Act in the US case, this makes them behave

[49] Office of the Press Secretary, "President Signs USA PATRIOT Improvement and Reauthorization Act," *Georgewbush-Whitehouse.archives.gov*, last modified March 9, 2006, http://georgewbush-whitehouse.archives.gov/news/releases/2006/03/20060309-4.html (accessed on 24.04.2016).

[50] Julian Hattem, "Obama Signs NSA Bill, Renewing Patriot Act Powers," Text, *Thehill*, last modified June 2, 2015, http://thehill.com/policy/national-security/243850-obama-signs-nsa-bill-renewing-patriot-act-powers (accessed on 28.05.2016).

[51] Jef Huysmans, "Minding Exceptions: The Politics of Insecurity and Liberal Democracy," *Contemporary Political Theory* 3, no. 3 (December 2004): 336.

awfully like non-democratic regimes. In addition, matters get even more serious if we consider that the proclaimed post-9/11 state of emergency from 2001 was once again prolonged last year by the US government.[52] Hence, for the past fifteen years, the USA as one of the most democratic countries in the world is under a perpetual state of emergency that allows the government to undertake extreme actions on a regular basis without wide popular consent. Put simply, originally labeled exceptional measures became the practice of normal politics over time. Huysmans outlines this as a paradox that happens when "security knowledge and technology that is meant to protect liberal democracy against violence seriously risks to undermine it".[53]

On the other hand, in the Chinese case the legislations from the very beginning had one primary goal – to preserve regime stability and social order. Since the legislations were introduced very early when the cyberspace technology was just emerging, the authoritarian CCP government had enough time to practically shape the local 'rules of the game' regarding the internet. According to Shanthi Kalathil and Taylor Boas, "[t]hrough measures ranging from blunt punitive actions to the subtle manipulation of the private sector, the Chinese state has been largely successful to date in guiding the broad political impact of Internet use".[54] These kind of regulations allowed the Chinese government to even censor and block some of the major companies as Google, Facebook, and Twitter from their network as they did not comply with the imposed rules. Rebecca MacKinnon suggests that China managed to adjust to the new digital age through what she calls the "networked authoritarianism", the situation in which the leading regime just nominally provides the internet freedoms to the public, while at the same

[52] Office of the Press Secretary, "Message - Continuation of the National Emergency With Respect to Certain Terrorist Attacks," *Whitehouse.gov*, last modified September 10, 2015, https://www.whitehouse.gov/the-press-office/2015/09/10/message-continuation-national-emergency-respect-certain-terrorist (accessed on 28.05.2016).
[53] Huysmans, "Minding Exceptions," 322.
[54] Shanthi Kalathil and Taylor C. Boas, *Open Networks, Closed Regimes: The Impact of the Internet on Authoritarian Rule* (Washington, DC, USA: Carnegie Endowment for International Peace, 2003), 40.

time remains in full control and removes perceived online threats to the leadership by using the national legal system as a main tool in that process.[55]

Overall, observing the legal provisions from the US and China case, it is clear that most of them prescribe and authorize the actions that can be, in regular terms, understood as controversial and way beyond the line of "normal politics". Additionally, both of these security issues were, as we will see in the next chapter, communicated in their own way depending on the political context and ultimately accepted by the audience. Hence, there is clear evidence that in both cases cyberspace was essentially securitized. Moreover, examining the empirical cases from the Copenhagen School's theory perspective, it is easily noticeable that the national governments of the US and China represent the securitizing actors, while the targeted audience is depicted in a form of general public living and operating within the borders of the two countries. Yet, what is not apparent at the moment is the way how the securitizing messages in the two cases are constructed in terms of the existential threat to the referent object, and how they are transmitted to the audience. As already mentioned in the previous sections, if a significant difference in the securitizing procedure does exist due to the difference in regime types, the reasonable expectation is to find it in how these messages are framed and disseminated. In order to investigate the potential differences, by using the qualitative content analysis and Vuori's five strands of securitization framework, I will now analyze the core justifications regarding the examined legislative acts provided by the two governments.

[55] Rebecca MacKinnon, "China's 'Networked Authoritarianism,'" *Journal of Democracy* 22, no. 2 (2011): 33.

Chapter 3 – The Justification Framing and Differing Practices Across Political Contexts

3.1 The Patriot Act and Vuori's Five Strands

The most prominent governmental justifications of an evident cyber securitization under the Patriot Act in the US case, came from three separate, yet equally important sides. The first one was from the US Congress (the Senate and the House of Representatives) members and committees who prepared, debated, and voted on the passing of the Act; the second one was from the US President George W. Bush who officially signed the Act into law; and the third one was from the US Department of Justice who guaranteed the constitutional conformity and fair enforcement of the Act's provisions. Overall, after conducting an in-depth text analysis of the corresponding primary sources, the transmitted messages to the target audience can be classified into four broad categories emphasizing: 1) the new tools at disposal to the government agencies responsible for the country's security; 2) the balance of the legislation in terms of security vs. freedom; 3) the war on terrorism; 4) the protection of Americans, civil liberties and way of life. In certain cases, the individual securitizing messages fit several of these categories at the same time, which empirically demonstrates Vuori's claim that securitization is a complex act that can carry at the same time many perlocutionary intentions. Consequently, beside the message itself (i.e. securitizing cyberspace), it is also important to examine the choice of words used in framing the messages as well.

From the securitization theory framework, by examining the speeches regarding the Patriot Act provided by three separate actors representing the US government, it is obvious that there is a unanimous consensus about the existential threat. In this case it is a threat of terrorism, and this can be seen from the following statements:

> “The anti-terrorism bill [Patriot Act] will provide law enforcement officials responsible for protecting American citizens with the intelligence information and the powers they need to prevent terrorist attacks, respond to attacks when necessary, and bring terrorist criminals to justice (Representative Skelton)”.[56]
>
> “Today, we take an essential step in defeating terrorism, while protecting the constitutional rights of all Americans (President Bush)”.[57]
>
> “Congress simply took existing legal principles and retrofitted them to preserve the lives and liberty of the American people from the challenges posed by a global terrorist network (the Department of Justice)”.[58]

Similarly, there is a common view concerning the referent object as well. Here, the dominant opinion is that America and American people are under imminent threat imposed by terrorists. The examples of such statements are the following:

> “It's imperative to provide our law enforcement agencies with the necessary tools to help protect Americans and prevent the types of cowardly acts that were committed against our great nation on September 11 (Senator DeWine)”.[59]
>
> “The elected branches of our government, and both political parties, are united in our resolve to fight and stop and punish those who would do harm to the American people (President Bush)”.[60]
>
> “[T]he Patriot Act has played a key part - and often the leading role - in a number of successful operations to protect innocent Americans from the deadly plans of terrorists dedicated to destroying America and our way of life (the Department of Justice)”.[61]

Briefly analyzing the sampled material, it is evident that the goal of the US administration was to persuade the audience how terrorism, as a serious war-like threat, is menacing the American nation and its core values. Hence, this danger had to be decisively repealed, fought, and

[56] The Department of Justice, “Congress Explains the USA PATRIOT Act,” *Justice.gov*, https://www.justice.gov/archive/ll/subs/q_support.htm (accessed on 21.04.2016).
[57] Office of the Press Secretary, “President Signs Anti-Terrorism Bill,” *Georgewbush-Whitehouse.archives.gov*, last modified October 26, 2001, http://georgewbush-whitehouse.archives.gov/news/releases/2001/10/20011026-5.html (accessed on 23.04.2016).
[58] *The USA PATRIOT Act: Preserving Life and Liberty* (Washington, DC: The Department of Justice, 2001), 1, https://www.justice.gov/archive/ll/what_is_the_patriot_act.pdf (accessed on 21.04.2016).
[59] The Department of Justice, “Congress Explains the USA PATRIOT Act.”
[60] Office of the Press Secretary, “President Signs Anti-Terrorism Bill.”
[61] *The USA PATRIOT Act: Preserving Life and Liberty*, 1.

defeated by granting the enhanced tools to the government intelligence and law enforcement agencies. And all of this was possible through the Patriot Act, the exceptional legislation which increases security of the country without hampering the constitutional rights of citizens. Nevertheless, despite the fact that the statements from three actors representing the US administration essentially carried the same message, and even used the same words and phrases in the process, the way how these messages were framed and disseminated differ significantly. In order to identify these dissimilarities, I will apply the theoretical framework of Vuori's five strands.

In the case of the securitizing messages originating from the US Congress, according to Vuori's theory, we can isolate two types of communication. Due to the very nature of any Congressional debate and the members' reflection on it, the most dominant types of messages transmitted to the audience are "claims" and "warns" followed by "urge" or "request" for some sort of action. The examples of the claims are the following:

> "I strongly support this important counter-terrorism bill because it will give law enforcement officials the flexibility and resources to eradicate acts of terrorism (Senator Baucus)";
>
> "This bill maximizes law enforcement's ability to locate criminals through surveillance and wiretapping provisions and helps intelligence communities to coordinate information sharing on terrorist activity (Senator Santorum)".[62]

Clearly, both statements communicate the message claiming the facts about the Patriot Act that could be reasonably believed or justified, but might not be obvious to the public. Similarly, the warnings highlight and remind the public about the present threat that needs to be tackled, as in the following examples:

[62] The Department of Justice, "Congress Explains the USA PATRIOT Act."

> “The laws that protect us must be relevant to the dangers that threaten us (Senator Hagel)”;
>
> “[T]he scourge of terrorism is going to be with us for a while (Senator Schumer)”.[63]

Additionally, the claim-warn sequence of securitizing messages by the Congress was most commonly followed by the mentioned urge or request for action by the Administration. In this case, it was call for support in order to pass the Patriot Act, exemplified by the following speeches:

> “Our goal must be stopping terrorists […] rather than wasting time, energy and resources fighting bureaucratic legal hurdles (House Speaker Hastert)”;
>
> “We're at war, and we need to give those who are fighting it the tools they need to win (Representative Pitts)”.[64]

Considering the examined sequence and the nature of the messages (i.e., directives; future oriented; can be argued) overall communicated by the Congress, according to Vuori’s framework we have a case of two types of securitization strands utilized in the process – “raising an issue to the agenda” and “legitimating future acts”. These types of communication were most probably crucial to fully convince the public of the necessity and legitimacy of the Patriot Act.

Conversely, in the case of speech delivered by President Bush, the message was framed in a slightly different manner. Naturally, the speech act structure contained both “claim” and “warn” parts. This can be noticed in the following sample:

> “We've seen the enemy, and the murder of thousands of innocent, unsuspecting people. They recognize no barrier of morality. They have no conscience. The

[63] Ibid.
[64] Ibid.

> terrorists cannot be reasoned with. […] Surveillance of communications is another essential tool to pursue and stop terrorists (President Bush)”.[65]

Evidently, the aim of the statement was to justify the enhanced electronic surveillance under the Patriot Act as a crucial and legitimate tool (i.e., claim) in a fight against the unconventional enemy (i.e., warn). However, unlike the Congress case, here the securitizing message sequence was followed by a declarative statement that had a goal to authoritatively establish the Patriot Act as something that will prevent any similar atrocities like the 9/11 events to happen ever again. Such declaration can be noticed in the following statement:

> “This legislation is essential not only to pursuing and punishing terrorists, but also preventing more atrocities in the hands of the evil ones. This government will enforce this law with all the urgency of a nation at war. (President Bush)”.[66]

From Vuori’s theory perspective, this type of speech act framing falls into the category of “securitization for deterrence”. From the Patriot Act angle, since the message was transmitted by a supreme authority within the country, the legitimization of the ongoing securitization was even further enforced.

Furthermore, although the bill was already in force for some period of time, the justification of enacting the controversial provisions under the Patriot Act did not stop. The Department of Justice provided what Vuori classified as “legitimating past act” or “reproducing securitization”. As in the previous two cases, the speech act sequence also contained the claim-warn structure of similar content, but here it was followed by assertive explanatory statements and empirical examples of results under the enacted legislation. These kind of messages can be summarized with the following one:

[65] Office of the Press Secretary, “President Signs Anti-Terrorism Bill.”
[66] Ibid.

> "The government's success in preventing another catastrophic attack on the American homeland since September 11, 2001, would have been much more difficult, if not impossible, without the USA Patriot Act (the Department of Justice)".[67]

Due to the controversial provisions contained in the Patriot Act, by reflecting on the positive effects that came as a result from enacting the bill, the US Administration wanted to show to the audience that the enhanced electronic surveillance measures were highly effective, while at the same time that they were not abused in any possible way.

In addition, if we examine the two previously mentioned acts concerning the cyber and homeland security from 2002, we will see the very same justification procedure, involving the three entities transmitting the messages corresponding to the strands of securitization characteristic for each of the actors as in the outlined case of the Patriot Act. In other words, out of five strands of securitization proposed by Vuori's theoretical framework, different empirical cases from the US on cyberspace securitization show that four of them were repetitively conducted in a manner consistent with the author's concept. Moreover, if we also include the proclamation of the state of emergency by President Bush as one of the starting points that contributed in the process of enacting the Patriot Act, then even the fifth strand labeled as "securitization for control" was utilized in the process. Therefore, considering the above stated facts, we can confidently claim that Vuori's five strands of securitization framework continually performs well when applied in a democratic context.

3.2 The "White Papers" and Conceptual Problems

On the other hand, the Chinese case exhibits considerably different characteristics. First of all, since the majority of the decisions are made within the leading bodies of the CCP, it is

[67] *The USA PATRIOT Act: Preserving Life and Liberty*, 4.

important to note that public debate of any sort is highly limited or even nonexistent. Moreover, since the national constitution allows the CCP to exercise measures that might be perceived (at least in the liberal-democratic sense) as beyond politics on a regular basis, the official justification of such acts is either redundant or unnecessary to be done in advance. However, knowing that securitization does exist in the authoritarian systems, this is not to say that appropriate justification of the securitizing acts to the public does not exist. For example, writing about the internet regulation from 1997, the New York Times reporter pointed out that the Chinese government organized a newspaper conference regarding the enacted law, but the "foreign journalists were not invited".[68] Hence, very limited amount of official government information is actually available for the wider (international) public. Yet, the Chinese government has a practice to periodically publish thematic "White Papers" that aim to concisely explain and legitimize legislations and strategies concerning a particular sector. In that light, partially influenced by external criticisms and accusations regarding the restrictive cyber policy, the "White Paper" entitled "The Internet in China" was published in 2010 with the objective to introduce "the facts of the Internet situation in China […] to the Chinese people and the peoples of the rest of the world".[69]

In sections IV and V, the government paper on internet is referring to the extensive list of cyberspace regulations since 1994, which represents a very rare and valuable source of official justifications for the mentioned legislations. The overall arguments used in the report can be allocated into three broad categories: 1) the irreplaceable role of internet for China; 2) the law based administration, rational application, spread, and sovereignty of internet; 3)

[68] Erik Eckholm, "China Cracks Down on Dissent in Cyberspace," *The New York Times*, December 31, 1997, sec. World, http://www.nytimes.com/1997/12/31/world/china-cracks-down-on-dissent-in-cyberspace.html (accessed on 15.05.2016).
[69] Information Office of the State Council of the PRC, *The Internet in China*, Government White Paper (Beijing: The State Council of the People's Republic of China, June 8, 2010), sec. Foreword, http://china.org.cn/government/whitepaper/node_7093508.htm (accessed on 09.05.2016).

guarantee of public freedoms/rights on internet. From the securitization theory perspective, the existential threat is vaguely defined as "all types of network crimes".[70] Again, this ambiguity leaves space for broader interpretation of security issues by the government, consequently permitting a wide range of appropriate responses to prevent these threats. In terms of the referent object, from the title of section V we can see that it is depicted in a form of internet security. However, as we could understand from the previous section, the internet security is tightly linked with the concept of national security through law, and implicitly to the regime security and social order. This view is even further enforced with numerous emphasis on the irreplaceable role of internet development and security for "national economic prosperity and development, state security and social harmony, state sovereignty and dignity, and the basic interests of the people".[71]

Considering that the "White Paper" is predominantly talking about the facts generated by the past events and supported by historical data regarding the internet governance in China, from Vuori's theory perspective this could only mean that the message disseminated by the government to the target audience was done in a form of "legitimating past act or reproducing securitization" strand, as this is the only strand related to the past. However, this is not entirely the case. The first major peculiarity that can be identified from the text is that it contains only one speech act that can be perceived as the necessary "warn". Since the lengthy government report has six body sections in summary, out of which two (IV and V) are directly and the other two (III and VI) indirectly speaking about the national internet security, this fact is even more surprising. Yet, the claim-warn-explain speech act sequence distinctive for the mentioned strand of securitization does exist, and it states the following:

> "Internet security is a prerequisite for the sound development and effective utilization of the Internet. Internet security problems are pressing nowadays, and

[70] Ibid., sec. IV. Basic Principles and Practices of Internet Administration.
[71] Ibid., sec. Foreword.

> this has become a problem of common concern in all countries. China also faces severe Internet security threats. Effectively protecting Internet security is an important part of China's Internet administration, and an indispensable requirement for protecting state security and the public interest”.[72]

With this speech act, the government clearly wanted to explain the logic behind the extensive internet regulation by numerous laws and protocols from the list that was presented in the following paragraph of the document and in section IV of the governmental report. Also, the assertive tone of the last sentence, characterized by use of the “Internet administration” term rather than control or censorship, perfectly matches Vuori’s “legitimating past act” strand.

However, beside the assertive explanatory speech act, the message further builds on the established claim-warn basis. The communication sequence is continued by a set of very authoritative declaratory statements:

> “The Chinese government believes that the Internet is an important infrastructure facility for the nation. Within Chinese territory the Internet is under the jurisdiction of Chinese sovereignty. The Internet sovereignty of China should be respected and protected”.[73]

Regarding the message itself, the Chinese government obviously wanted to deter the emerging external criticism and to justify their strict regulatory practices of the cyberspace by framing it as a part of their national internet sovereignty. The use of the term “sovereignty”, in combination with internet, on its own prescribes use of enhanced security measures if endangered in any possible way. As from the five strands perspective, the above statement does not fit any of the established categories. Although the message partially tries to legitimize regulations and practices from the past, as we could see in Chapter 1, due the declarative nature of the statement it does not fulfill the prescribed conditions for “legitimating past act /

[72] Ibid., sec. V. Protecting Internet Security.

[73] Ibid.

reproducing securitization" strand (i.e., explain-assertive-legitimacy-past-argued). Conversely, although carrying such message, the examined speech cannot be regarded as "securitization for deterrence" strand due to the reference to the past acts instead of the future ones. Hence, if we would blindly follow the guidelines from Vuori's framework, we would interpret the given statement as one attempting to legitimize the past act by deterring the future one. Evidently, outside of a democratic context, it is possible to make a declarative statement that sets the 'new rules of the game' while at the same time retrospectively legitimizing the conducted acts. Thus, Vuori's framework needs to be updated with a new "cross-temporal declaration" strand.

Then again, this is not the end to conceptual problems of Vuori's theory in Chinese case. Immediately after the declarative statements, the speech act sequence is continued by a firm set of directives requiring the following:

> "Citizens of the People's Republic of China and foreign citizens, legal persons and other organizations within Chinese territory have the right and freedom to use the Internet; at the same time, they must obey the laws and regulations of China and conscientiously protect Internet security".[74]

As it can be easily noticed, the government here used its supreme authority and legal right to impose a strict obedience of the rules prescribed by laws and regulations regarding the cyberspace on territory of PRC. Put differently, the aim was to underline the fact that the legal system of a sovereign country must be undisputedly and indiscriminately respected everywhere in the world, regardless of political or any other contextual difference. Although the examined speech act contains most of the elements that can categorize it as the "securitization for control" strand, similarly to the previous example, the message cannot be classified as such due to the reference to legislative acts that were in force for a considerable amount of time, some of them even more than a decade. Yet again, the speech cannot be regarded as the "past act" one either

[74] Ibid.

due to its emphasized directive nature. Essentially, following Vuori's original conceptual propositions, we might have a hybrid message legitimating the past acts by requiring continuous obedience. Even though this theoretical anomaly might be revealing to us the hidden agenda of internet control in China, such conceptual construction was not foreseen by Vuori. Again, the new "recapitulation of authority" strand containing the outlined features needs to be added to the original framework.

Furthermore, recalling the Chapter 1, Searle and Vanderveken outlined the five elementary types of speech acts, out of which expressives and commissives were not applied in Vuori's framework. Although the expressives might be able to contribute, for example, in legitimizing the securitizing acts by thanking or praising the role of some prominent individual or institution in the process by utilizing their authority, personality cult, and/or expertise, this is highly debatable. On the other hand, since commissives pledge strong attachment to decisions and actions in any temporal context for a wide range of purposes, their omission from the proposed theoretical framework by Vuori is very surprising. In Chinese case, this type of communication was used in many occasions, the example is the following:

> "The basic goals of China's Internet administration are to promote general and hassle-free Internet accessibility, and sustainable and healthy development, guarantee citizens' freedom of speech online, regulate the order of Internet information transmission, promote the positive and effective application of the Internet, create a market environment for fair competition, guarantee the citizens' rights and interests vested in the Constitution and law, and guarantee safety for Internet information and state security".[75]

As it can be seen from the example, the frequent use of "guarantee" term has a goal to show a deep commitment of the Chinese government to protect its citizens and their rights. In other words, the message is framed in such a way that the continuously applied "internet

[75] Ibid., sec. IV. Basic Principles and Practices of Internet Administration.

administration" is in the citizens' best interest. In addition, the expressed pledge by the government in the speech act is not bound by any temporal boundaries. Hence, at the same time it is legitimizing the actions that were taken in the past and that will be done in the future. Although similar statements can be found in the US case as well, the speech acts framed in this way cannot be classified in the original Vuori's framework. Thus, the original framework needs a category that will accommodate the statements framed in the highlighted way.

Besides the frequent use of commissive statements ensuring a range of different freedoms to the citizens, the "White Paper" is also containing a lot of regular claims that are not part of any claim-warn-perlocution sequence. These statements were particularly present in sections I and II, and they transmitted some very affirmative messages to the audience regarding the internet in general. The examples are the following:

> "The Internet is helping promote the economic and social development of China. […] It has become an indispensable tool in people's life, work and studying, exerting a profound influence on every aspect of social life".[76]

Since they are not part of the elementary securitizing speech act sequence proposed by Vuori, according to established theoretical elements, these statements would not contribute much in dissemination of the overall securitizing message to the target audience. However, this is not entirely true, and such verbal acts might play a considerable role in the process, at least in the non-democratic contexts. For example, in Chinese case these speech acts had a goal to enforce the view of exceptional importance of the internet and its continuous development to the country. Consequently, the corresponding discourse directly influences the process of reproducing the idea of internet and cyberspace as a part of a core national interest and issue of national security. As we could see from the previous chapter, this claim served as a primary

[76] Ibid., sec. II. Promoting the Extensive Use of the Internet.

reason for cyberspace securitization in the first place. From this perspective, these statements seem to be very important elements of what also Vuori identifies and labels as "autocommunication" practice in the socialist systems.[77] Thus they need to be addressed in more detail.

To summarize, based on the inductive text analysis of the Chinese "White Paper", I would add three strands to Vuori's framework, as summarized in Table 2 below.

Table 2 - Additions to Vuori's Five Strands of Securitization

Strand of Securitization	**Elementary Speech Act**	**Illocutionary Point**	**Perlocutionary Aim**	**Temporality**	**Debate**
Cross-temporal Declaration	Claim, Warn, *Declare*	Declarative	Legitimacy	Past (and Future)	No
Recapitulation of Authority	Claim, Warn, *Request*	Directive	Obedience / Discipline	Past (and Future)	No
Commitment to Protect	Claim, Warn, *Commit*	Commissive	Legitimacy	Past and Future	No

Comparing the conducted analysis in China with the US one, the ultimate observation is that Vuori's concept performs considerably differently in dissimilar political contexts, particularly with regards to the issue of temporality. In other words, the "conceptual travel" of securitization theory under Vuori's five strands framework from democratic to non-democratic background, ultimately fails to deliver the intended results of providing the uniform analytical guidelines for both political systems that would break away from the "Westphalian straitjacket" issue. Paradoxically, it seems that Vuori's framework itself does not fully escape the Western

[77] Vuori, "Illocutionary Logic and Strands of Securitization," 71.

liberal-democratic bias in its analysis, which is empirically demonstrated on the example of perfect conceptual fit in the US case and problematic application in the Chinese case. Yet, this is not to say that the main idea of the five strands theory is bad, quite the contrary. Although it faces the outlined problems when applied in non-democratic contexts and thus requires more thorough conceptual revision, it is very helpful in revealing similarities, differences, and patterns in securitizing message framing between the two diverging political systems. From the analysis of cyberspace securitization, it is evident that such dissimilarities do exist between the US and PRC. However, in order to understand what type of dissimilarity is actually present, we must observe the major differences in technical procedure and speech act framing between the two cases in more detail.

3.3 The Differences in the Process of Cyber Securitization

While conducting my qualitative content analysis and examining the securitization message framing in the US and China through Vuori's five strands framework, I have identified a number of important differences in the process of securitization of cyberspace that clearly delineate the practices applied in democratic and authoritarian political regimes. Beside the variety of minor ones, I have grouped the major dissimilarities into four broad categories. As concisely presented in Table 3, these groupings are referring to: what caused the securitization process to occur (i.e., the trigger); who were the actors involved in the process; how was the threat constructed and represented over time; and what role did the national Constitutions and legislative frameworks of the two countries play in the cyber securitization procedure. In the following subsections, I will briefly reflect on each of these categories before summarizing what we can actually learn from them about securitization in diverging contexts.

Table 3 - The Key Differences in the Process of Cyber Securitization

Item	The US	The PRC
The Trigger for Securitization	Reaction to the Event	Proactive Practice
The Actors Involved	Multiple	Centralized
The Threat Construction	Evolving	Stable
The Reference to Law and Constitution	Restrictive Role	Permissive Role

3.1.1 The Trigger for Securitization

Although some sort of basic internet regulations and counter cyber-threat capabilities did previously exist in the US, the 9/11 terrorist attack was the ultimate trigger for the US Administration to deal with cyberspace threats in a more systematic way. According to Robert Latham, the September 11 attack "has galvanized and deepened attention to the relationship between IT and security".[78] Put differently, the extensive cyber securitization practices, along with corresponding political and scientific discourse supporting them in the US, were initiated by the 9/11 events. Taking this into consideration, we can classify these securitizing acts as reactive (i.e., reaction to the event), which is quite logical for the democratic systems as the governments need a sufficiently good reason to legitimize their extreme measures to the target audience in such political contexts. In this case, the September 11 attacks served to unite the public in positive opinion regarding the proposed enhanced electronic surveillance measures,

[78] Robert Latham, "Introduction," in *Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security*, ed. Robert Latham (New York: The New Press, 2003), 1.

which in a regular state of affairs would be highly unlikely to be accepted by the US citizens. The similar reasoning stands valid for most of the democratic systems in the world.

On the other hand, the Chinese case of cyber securitization exhibits a completely different approach. Since the imposed measures and the appropriate discourse were present even before the internet and information technologies displayed their full capabilities in the early 1990s, the governmental actions can be perceived as proactive (i.e., preemptive). Reflecting on this phenomenon, Greg Austin pointed out that “China’s leaders had prepared their defenses for this information explosion long ago”.[79] Similarly, by examining the attitude of the leadership towards internet from the very beginnings, Zixue Tai explains that “the authoritarian regime has been quite wary of the potentially destructive nature of a brand-new information environment brought about by ICTs”.[80] In addition, if we compare the examined legislations from 1994 and 1997, it is clear that the former gives very vague regulatory guidelines, while the later one prescribes more specific restrictions. This shows that although Chinese government could not fully predict the effects of the new technology, it preemptively securitized it and then progressively increased the measures as the perceived risks became more evident over years. Hence, the empirical case of cyber securitization in China is possibly showing us the very core logic behind the overall securitization practices in the authoritarian regimes.

3.1.2 The Actors Involved

In the US case, we can observe a very peculiar pattern of diffused cyber securitization process in which the speech act is communicated by the three separate entities representing a single unit – the US government. In addition, it seems that these entities also have a distinct

[79] Greg Austin, *Cyber Policy in China*, China Today (Cambridge, UK: Polity Press, 2014), 62.
[80] Zixue Tai, *The Internet in China: Cyberspace and Civil Society*, 1st ed., Routledge Studies in New Media and Cyberculture (New York: Routledge, 2006), 116.

role in communicating the intended messages to the audience. In this procedure the Congress can be broadly understood as the one aiming to raise the issue and legitimizing the potential securitizing act, the president's speech can be perceived as the one declaring the state of affairs and enforcing the security issue at hand, while the Department of Justice, in addition to numerous hearings regarding the subject, is the one aiming to legitimize the results of the securitizing act or reproducing its status. Since this procedure is very common, if not identical, in the process of enacting laws regarding the national security issues in the US, we can understand this dispersed speech act transmission as something that I would label as "the US securitization cycle". Despite the fact that this kind of diffused securitization process might differ in terms of institutions involved across the democratic context in general, the ideas of transparency, legitimacy, accountability and shared competencies essentially present in the US case is something characteristic for all democratic political systems.

Contrariwise, due to the lacking or very limited public debate, it seems that in China we have a very centralized framework where the government (i.e., the CCP) is the ultimate decision maker and transmitter of the securitizing messages. However, as it could be seen from the case study, the public debate is highly limited and the decision-making process is nontransparent. According to Austin, the reason for this limited access to information is due to the "closed nature of its political system, the lack of reporting on what the leaders say in private, and the high political cost for its leaders of being seen to be diverging from the leadership consensus".[81] Put differently, the centralized voice of the Chinese government has an aim to enforce the undisputed authority of the regime, while at the same time to express the unanimous agreement regarding the decisions that are made for the sake of regularly emphasized political and social stability in the country. For the above stated reasons, unlike in the US case, there is

[81] Austin, *Cyber Policy in China,* 8.

no need for continuous and extensive justification of the decisions made by the government, as most of them are done in a form of directives that cannot be publically disputed. Needless to say, such and similar approaches are very common, if not even typical, for non-democratic regimes.

3.1.3 The Threat Construction

Concerning the definition of threat, the US case demonstrates a fair amount of adaptability over the analyzed period of time from 2001 until 2006. Obviously, due to the events that actually triggered the process of cyber securitization, the main and repetitive threat reference was to terrorism and terrorists, especially in the context of new challenges due to the continuous developments in technology. Beside the always present terrorism, the report supplementing the "Cyber Security Enhancement Act of 2002" bill proposal also outlined common criminals as a part of the threat, while mentioning the terms such as cybercrime and cyberterrorism as well.[82] Similar rhetoric was later used in the process of supporting the Patriot Act reauthorization in 2005-2006. Moreover, on top of the identified dangers, the report accompanying "Homeland Security Act of 2002" bill added the threat of "other nations" to the agenda.[83] This threat later reappeared in forms of "America's enemies" and "foreign powers" in many official documents throughout 2002-2005 period. Finally, the "Reauthorization Act" that was signed into law in 2006 is quite surprisingly adding the threat of methamphetamine, which even got a special attention in the President's speech.[84] Thus, considering the stated material, it is evident that the idea of threat progressively evolved over time in the US. Again,

[82] James Sensenbrenner, *Cyber Security Enhancement Act of 2002*, House Report 107-497 (Washington, DC: House of Representatives - Judiciary Committee, June 11, 2002), 8–9, https://www.congress.gov/107/crpt/hrpt497/CRPT-107hrpt497.pdf (accessed on 22.04.2016).

[83] Richard Armey, *Homeland Security Act of 2002*, House Report 107-609 (Washington, DC: Select Committee on Homeland Security, July 24, 2002), 63, https://www.congress.gov/107/crpt/hrpt609/CRPT-107hrpt609-pt1.pdf (accessed on 22.04.2016).

[84] Office of the Press Secretary, "President Signs USA PATRIOT Improvement and Reauthorization Act."

this is highly connected to the previously outlined "reactivity" of the democratic systems, the practice where the threats are only securitized when clearly identified and for a good reason.

Conversely, the Chinese case exhibits a very stable notion of the online threats over time. Since the law prescribed from the very beginning that any use of computers and information networks in a way that endangers the state interests represents a crime, in that light the threat was perceived as all types of computer/network crimes. However, it is important to remember that the term "threat" is almost not used at all, unlike in the US case where it is intensively exploited. This can be interpreted in a way that the Chinese government, as the main provider of security and stability for the country and its citizens, is doing a good job in deterring the dangers present out there, hence the threats are eliminated and the society should not worry about these problems. From this point of view, the frequent reference to different types of threats would mean that the government is not coping with these security issues effectively, which would diminish the legitimacy of the leadership. Moreover, the important difference between the US and Chinese case is that in the former one we have reference to both internal (e.g., crimes) and external dangers (e.g., terrorism, foreign powers), while in the later there is only reference to internal issues (e.g., network crimes). In opposition, the message in the US case is intended exclusively to internal audience, while in the Chinese case it is explicitly stated that it is for both internal and external audience, which is also evident due to the fact that the "White Paper" was officially published in English.

3.1.4 The Reference to Law and Constitution

When referring to the established legal systems within their countries, the two governments display a quite different approach. In the US case, due to the characteristic democratic legacy, the big part of justifying the extreme measures is done on the account that they are not going to breach the constitution and all the rights and freedoms granted to the citizens under this supreme legal act. In other words, the constitution is presented as an ultimate safeguard that will prevent the abuse of power granted to the government by the controversial bills. In the Chinese case, the national constitution itself prescribes the use of enhanced measures as if they are the most normal thing. Consequently, the imposed enhanced measures are legitimized by referring to the law and constitution as something that cannot be negotiated and that must be respected. Put differently, the constitution as the highest legal act of the country, on its own represents the major justifying argument of the authoritarian regime in China. Considering the above mentioned, what can be noticed from the two cases is the fact that the constitution and corresponding laws play a rather restrictive role in the democratic context, while in the non-democratic background they have a permissive role. Nonetheless, they are both used in legitimizing the actions in their own separate ways depending on the regime type.

3.1.5 The Takeaways from Conducted Analysis

Overall, examining the results of the conducted qualitative content analysis and application of Vuori's five strands framework across differing political contexts described in the cases of China and the US, we can understand several things regarding the regime types and securitization. The main empirical finding is that securitization ultimately can occur in both political contexts, yet the core approach to doing so differs based on the regime type. Put differently, the demonstrated differences in this section are not only dissimilarities between the examined empirical cases *per se*, but they are critically linked to the specific regime types of these cases in general. Hence, in the case of timing of the speech act, in the democratic US context we could see that the securitizing message is commonly disseminated in advance to the securitizing act as a prerequisite for the audience to accept it, while reflection on the conducted act is only done in order to enforce or relegitimize it. On the other hand, in the authoritarian Chinese case, we could see that justification for securitizing acts can happen at any time suitable for the leadership's interests, such as when the regime's legitimacy is challenged. The fact that the government's "White Paper" from 2010 was published in English could be seen as a response to the international challenges concerning the Chinese internet policy. Also, what distinguishes the Chinese case is that, regardless of the timing of the securitizing speech act, the audience must undisputedly accept the acts in any case.

Furthermore, the structure of the political power is considerably different between the two contexts - decentralized in democracy, and highly centralized in non-democracy. The decentralized system is observable in the US, notably on the division of responsibilities between several institutions representing the government, accompanied by higher transparency and accountability in the policy making process. Conversely, in the non-democratic Chinese context, the political power is clearly concentrated in the hands of only one institution - the CCP, and any internal divisions are less visible to the public or anyone outside the party. Moreover, the empirical cases highlighted the tendency of democratic states to pursue the extreme measures as a mean of last resort in reaction to the imminent threat, while in non-democracies these measures are part of regular practice in preemptive deterrence of the potential threats. Deriving from this, the empirics revealed more precise and adaptive identification of threats in the US, while in China this construction remained more vague and stable through time. Consequently, it is clear that the constitution in democratic context has restrictive and safeguarding role, while in authoritarian system it has permissive and legitimating role concerning the enhanced measures. Therefore, the empirical analysis of cyberspace securitization in the US and China not only reveals the dissimilarities between the two cases, but it also demonstrates the general trends and differences between the democratic and authoritarian regimes and their securitizing practices.

Conclusion

Inspired by the existing academic debate in the field of security studies on the topic of securitization theory and different political contexts, my research aimed to explore the following two things: 1) whether the securitization occurs in both political regimes; and 2) in case it does exist, whether there are any core differences in the process between these two diverse political contexts. Informed by the existing literature on the topic and the empirical analysis of the regulations of cyberspace in the USA and China, I have argued that: securitization does happen in both political regimes; the long-term state of emergency can cause the democratic regimes to create a policymaking environment resembling that of authoritarian regimes; the difference between the securitization procedure in the democratic and non-democratic political context does exist and it can be clearly visible in the way how securitizing messages are framed and transmitted through the speech act to the target audience; and Vuori's framework based on the illocutionary logic for cross-contextual comparison of the securitization process is insufficient to fully analyze the securitizing acts in the non-democratic political settings in its original form.

Supported by the comprehensive and systematic qualitative content analysis and Vuori's five strands of securitization framework, the investigation of the empirical data has ultimately validated all the above presented claims. The securitization in both political contexts was confirmed by examining the controversial provisions entitled "The Enhanced Electronic Surveillance" under the Patriot Act in the US case, and regulations provided by 1994 and 1997 laws in Chinese case, along with the corresponding official justifications for enacting these legal acts disseminated by the respective governments. Moreover, the perpetual prolongation of the post-9/11 state of emergency in the US case demonstrates that the government retained the capability of pursuing the political actions without following the traditionally established liberal-democratic rules and guidelines, regardless of the fact whether this possibility is utilized (i.e., abused) or not. Furthermore, by examining and comparing the securitizing speech acts over time both within and across political contexts, the empirical analysis has revealed that the securitization procedure between the democratic and authoritarian regimes differs in terms of the trigger for securitization (reactive vs. proactive), the securitizing actors involved (multiple vs. centralized), the threat construction (evolving vs. stable), and in reference to the law and constitution (restrictive vs. permissive role). And finally, the empirics have shown that Vuori's concept perfectly matches the democratic context, but when applied in the non-democratic one, it faces the conceptual problems due to the absent "cross-temporal declaration", "recapitulation of authority", and "commitment to protect" strands of securitization that were not identified in the original framework.

Taking the above mentioned into consideration, this research contributes to the broader literature in several different ways. First of all, it embarks on a challenging comparative analysis of the process of securitization in two contrasting political regime types within a single project, which is very rare in the existing literature on the topic. Moreover, it contributes to the ongoing academic debate regarding the topic of contextualization of securitization by empirically demonstrating that securitization does take place in both democracies and non-democracies. In that light, this research also contributes to the mentioned debate by providing new and specific insights regarding the dissimilarities of the securitizing acts between the two differing political regimes. Additionally, by focusing on the underexplored substance of the speech act (i.e., the language used in message framing) rather than on a mainstream debate regarding its conceptual appropriateness in different contexts, the conducted study contributes to the academic discussion by introducing the new ideas on top of Vuori's findings on the same topic. And lastly, the research contributes to the wider literature by testing and improving

Vuori’s original five strands of securitization framework by applying it in both political regime type settings.

However, my research also faces a variety of limitations. First of all, due to the very nature of the authoritarian regime in China, the political debate on variety of topics is either nonexistent or remains within the inner circle of the CCP leadership. Hence, the official primary data on the examined topic was very hard to obtain and thus remained very limited. Yet, this is the reality on the ground that every researcher needs to face when analyzing the Chinese political context and an inherent feature of this regime type. On the other hand, even if the primary data was provided by the government, it was commonly available only in Chinese language and thus out of my capability of interpretation. Consequently, the amount of data processed in my research is highly unbalanced in favor of the transparent US case. Deriving from this, if we do not consider conceptually analogous legislative documents, my research faced an issue of comparability of the examined material. These issues would arise, for example, if the data originating from the US President’s speech would be compared with the parts of the Chinese government’s “White Paper” report. Reflecting on this issue, I do not maintain the illusion that such data is direct equivalent to one another, however it is comparable on the ground of having the same purpose – to transmit a securitizing message to the audience. Also, due to the limited time and length of my study, I was unable to examine both alternative actors that could significantly participate in the process (e.g., media, elites, NGOs, corporations), and some additional cases of cyber securitization across the two political contexts. Both would significantly help me in drawing much stronger conclusions on the examined topic.

In that light, my research also provides a good basis for further studies on the topic. As it was just mentioned, the investigation of the alternative actors and their role in the process of securitization, along with additional cases of securitization in both democratic and non-democratic political contexts would possibly provide a much clearer picture of the examined issues and even further contribute to the academic debate on the contextualization of securitization. Moreover, it would be very interesting to observe the process of securitization in the context of the so called "competitive authoritarian regimes". According to Steven Levitsky and Lucan Way, these regimes are "civilian regimes in which formal democratic institutions exist and are widely viewed as the primary means of gaining power, but in which incumbents' abuse of the state places them at a significant advantage vis-`a-vis their opponents".[85] Evidently, these hybrid political regimes would give new insights regarding the topic, especially concerning the legitimizing speech acts. Similarly, the investigation of the cyber-securitizing practices and their development over time in the US case could also provide some very important insights for the broader field of security studies. This claim is based on the observable data regarding the cybersecurity bills that entered into force recently, which involve peculiar justifications and threat constructions that resemble characteristics of the concept known as the "riskification" rather than the ones typical for securitization.

Overall, from the presented material we can conclude that securitization as a concept plays equally important role in both political contexts. Although the motivations and approaches in applying its postulates do exist if we 'travel' across the differing regime types, the fact is that securitization has one universal role regardless of the political regime – to secure the issues designated by the actors in power. As we could see from the comparative empirical analysis presented in this research, cyberspace generally became a very active ground for different types of securitization in both democratic and non-democratic settings, and this trend will continue in the future as well. The reason for such claim is very simple and intuitive. The

[85] Steven Levitsky and Lucan A. Way, *Competitive Authoritarianism: Hybrid Regimes after the Cold War*, Problems of International Politics (New York: Cambridge University Press, 2010), 5.

more the cyberspace technology develops, the more people utilize it and depend on it. And the more the public depends on it, the more it becomes perceived as the security issue. Consequently, the more widely it is perceived as the security issue, the easier it is for the policymakers to impose and legitimize measures that might endanger some basic rights and freedoms. It is as simple as that. And this is not only concerning the cyberspace, but many other areas as well. Hence, we can see that people themselves subconsciously participate in the process of (re)producing these security issues. Thus, the logical question emerges – are we approaching the time when we will live in some sort of a perpetual state of emergency? Quite possibly, yes. Can we do something to prevent this trend? Quite possibly, no. Should we discuss it in academic circles? Definitely, yes. Therefore, I hope that my research on the topic made at least a modest step in direction of an overall understanding of this contemporary issue.

Appendix 1 – Title II of the Patriot Act

Section	Title	Section	Title
201.	Authority to intercept wire, oral, and electronic communications relating to terrorism.	202.	Authority to intercept wire, oral, and electronic communications relating to computer fraud and abuse offenses.
203.	Authority to share criminal investigative information.	204.	Clarification of intelligence exceptions from limitations on interception and disclosure of wire, oral, and electronic communications.
205.	Employment of translators by the Federal Bureau of Investigation.	206.	Roving surveillance authority under the Foreign Intelligence Surveillance Act of 1978.
207.	Duration of FISA surveillance of non-United States persons who are agents of a foreign power.	208.	Designation of judges.
209.	Seizure of voice-mail messages pursuant to warrants.	210.	Scope of subpoenas for records of electronic communications.
211.	Clarification of scope.	212.	Emergency disclosure of electronic communications to protect life and limb.
213.	Authority for delaying notice of the execution of a warrant.	214.	Pen register and trap and trace authority under FISA.
215.	Access to records and other items under the Foreign Intelligence Surveillance Act.	216.	Modification of authorities relating to use of pen registers and trap and trace devices.
217.	Interception of computer trespasser communications.	218.	Foreign intelligence information.
219.	Single-jurisdiction search warrants for terrorism.	220.	Nationwide service of search warrants for electronic evidence.
221.	Trade sanctions.	222.	Assistance to law enforcement agencies.
223.	Civil liability for certain unauthorized disclosures.	224.	Sunset.
225.	Immunity for compliance with FISA wiretap.		

Source: the Patriot Act[86]

[86] Sensenbrenner, *USA Patriot Act of 2001*, sec. Title II-Enhanced Surveillance Procedures (Sec. 201-225).

Appendix 2 – The Main Cyberspace Laws in PRC (1994-2005)

Name of the Legislation	Year
Regulations for Safety Protection of Computer Information Systems	1994
Computer Information Network and Internet Security, Protection and Management Regulations [Measures on the Administration of Security Protection of the International Networking of Computer Information Networks]	1997
Measures on the Administration of Internet Information Services	2000
Regulations on Telecommunications of the People's Republic of China	2000
Provisions on the Administration of Electronic Bulletin Services via the Internet	2000
Decision of the National People's Congress Standing Committee on Guarding Internet Security	2000
Provisions on the Administration of Foreign-funded Telecommunications Enterprises	2002
Law of the People's Republic of China on Electronic Signatures	2005
Provisions on the Administration of Internet News Information Services	2005

Source: "The internet in China" and Hirchina.org[87]

[87] Information Office of the State Council of the PRC, *The Internet in China*, sec. IV. Basic Principles and Practices of Internet Administration; "List of Chinese Laws," *Hirchina.org*, http://www.hrichina.org/en/list-chinese-laws (accessed on 29.05.2016).

Bibliography

Armey, Richard. *Homeland Security Act of 2002*. House Report 107-609. Washington, DC: Select Committee on Homeland Security, July 24, 2002. Accessed April 22, 2016. https://www.congress.gov/107/crpt/hrpt609/CRPT-107hrpt609-pt1.pdf.

Asian Legal Information Institute, tran. “Regulations of the People’s Republic of China for Safety Protection of Computer Information Systems.” *Asianlii.org*. Accessed April 7, 2016. http://www.asianlii.org/cn/legis/cen/laws/rfspocis719/.

Austin, Greg. *Cyber Policy in China*. China Today. Cambridge, UK: Polity Press, 2014.

Balzacq, Thierry. “The Three Faces of Securitization: Political Agency, Audience and Context.” *European Journal of International Relations* 11, no. 2 (June 1, 2005): 171–201.

Barthwal-Datta, Monika. “Securitising Threats without the State: A Case Study of Misgovernance as a Security Threat in Bangladesh.” *Review of International Studies* 35, no. 2 (2009): 277–300.

Buzan, Barry, and Richard Little. “Why International Relations Has Failed as an Intellectual Project and What to Do About It.” *The Millenium Journal of International Studies* 30, no. 1 (2001): 19–40.

Buzan, Barry, Ole Waever, and Jaap de Wilde. *Security : A New Framework for Analysis*. Boulder, Colorado: Lynne Rienner Publishers, 1998.

Deibert, Ronald J., and Rafal Rohozinski. “Risking Security: Policies and Paradoxes of Cyberspace Security.” *International Political Sociology* 4, no. 1 (2010): 15–32.

Eckholm, Erik. “China Cracks Down on Dissent in Cyberspace.” *The New York Times*, December 31, 1997, sec. World. Accessed May 15, 2016. http://www.nytimes.com/1997/12/31/world/china-cracks-down-on-dissent-in-cyberspace.html.

Elbe, Stefan. “Should HIV/AIDS Be Securitized? The Ethical Dilemmas of Linking HIV/AIDS and Security.” *International Studies Quarterly* 50, no. 1 (2006): 119–144.

Gardner, Hall. “War and the Media Paradox.” In *Cyber Conflict and Global Politics*, edited by Athina Karatzogianni, 13–30. Contemporary Security Studies. Taylor & Francis, 2008.

Gerschewski, Johannes. “The Three Pillars of Stability: Legitimation, Repression, and Co-Optation in Autocratic Regimes.” *Democratization* 20, no. 1 (January 1, 2013): 13–38.

Hansen, Lene. “The Little Mermaid’s Silent Security Dilemma and the Absence of Gender in the Copenhagen School.” *Millennium - Journal of International Studies* 29, no. 2 (June 1, 2000): 285–306.

Hansen, Lene, and Helen Nissenbaum. “Digital Disaster, Cyber Security, and the Copenhagen School.” *International Studies Quarterly* 53, no. 4 (December 1, 2009): 1155–1175.

Hattem, Julian. “Obama Signs NSA Bill, Renewing Patriot Act Powers.” Text. *Thehill*. Last modified June 2, 2015. Accessed May 28, 2016. http://thehill.com/policy/national-security/243850-obama-signs-nsa-bill-renewing-patriot-act-powers.

Huysmans, Jef. “Minding Exceptions: The Politics of Insecurity and Liberal Democracy.” *Contemporary Political Theory* 3, no. 3 (December 2004): 321–341.

Information Office of the State Council of the PRC. *The Internet in China*. Government White Paper. Beijing: The State Council of the People’s Republic of China, June 8, 2010. Accessed May 9, 2016. http://china.org.cn/government/whitepaper/node_7093508.htm.

Jackson, Nicole J. “International Organizations, Security Dichotomies and the Trafficking of Persons and Narcotics in Post-Soviet Central Asia: A Critique of the Securitization Framework.” *Security Dialogue* 37, no. 3 (September 1, 2006): 299–317.

Kalathil, Shanthi, and Taylor C. Boas. *Open Networks, Closed Regimes: The Impact of the Internet on Authoritarian Rule*. Washington, DC, USA: Carnegie Endowment for International Peace, 2003.

Latham, Robert. “Introduction.” In *Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security*, edited by Robert Latham, 326. New York: The New Press, 2003.

Legal Information Institute. “Electronic Surveillance.” *Cornell.edu*. Last modified July 17, 2008. Accessed May 3, 2016. https://www.law.cornell.edu/wex/electronic_surveillance.

Lehman, Lee & Xu, tran. “Computer Information Network and Internet Security, Protection and Management Regulations.” *Lehmanlaw.com*. Accessed April 7, 2016. http://www.lehmanlaw.com/resource-centre/laws-and-regulations/information-technology/computer-information-network-and-internet-security-protection-and-management-regulations-1997.html.

Levitsky, Steven, and Lucan A. Way. *Competitive Authoritarianism: Hybrid Regimes after the Cold War*. Problems of International Politics. New York: Cambridge University Press, 2010.

Library of Congress. “Summary of H.R.3162 - 107th Congress (2001-2002): Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001.” *Congress.gov*. Last modified October 26, 2001. Accessed April 23, 2016. https://www.congress.gov/bill/107th-congress/house-bill/3162/summary/81.

Linz, Juan José. *Totalitarian and Authoritarian Regimes*. London, UK: Lynne Rienner Publishers, 2000.

MacKinnon, Rebecca. “China’s ‘Networked Authoritarianism.’” *Journal of Democracy* 22, no. 2 (2011): 32–46.

Office of the Press Secretary. “Message - Continuation of the National Emergency With Respect to Certain Terrorist Attacks.” *Whitehouse.gov*. Last modified September 10,

2015. Accessed May 28, 2016. https://www.whitehouse.gov/the-press-office/2015/09/10/message-continuation-national-emergency-respect-certain-terrorist.

———. “President Signs Anti-Terrorism Bill.” *Georgewbush-Whitehouse.archives.gov*. Last modified October 26, 2001. Accessed April 23, 2016. http://georgewbush-whitehouse.archives.gov/news/releases/2001/10/20011026-5.html.

———. “President Signs USA PATRIOT Improvement and Reauthorization Act.” *Georgewbush-Whitehouse.archives.gov*. Last modified March 9, 2006. Accessed April 24, 2016. http://georgewbush-whitehouse.archives.gov/news/releases/2006/03/20060309-4.html.

Peters, Gerhard, and John T. Woolley. “George W. Bush: Proclamation 7463 - Declaration of National Emergency by Reason of Certain Terrorist Attacks.” *The American Presidency Project*. Last modified September 14, 2001. Accessed April 26, 2016. http://www.presidency.ucsb.edu/ws/?pid=61760.

Searle, John, and Daniel Vanderveken. *Foundations of Illocutionary Logic*. Cambridge, UK: Cambridge University Press, 1985.

Sensenbrenner, James. *Cyber Security Enhancement Act of 2002*. House Report 107-497. Washington, DC: House of Representatives - Judiciary Committee, June 11, 2002. Accessed April 22, 2016. https://www.congress.gov/107/crpt/hrpt497/CRPT-107hrpt497.pdf.

———. *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001*, 2001. Accessed April 23, 2016. https://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf.

Singer, Peter Warren, and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. What Everyone Needs to Know. New York, USA: Oxford University Press, 2014.

Swartz, Jon. “Stephen Hawking Opens up.” *Usatoday.com*. Last modified December 1, 2014. Accessed May 27, 2016. http://www.usatoday.com/MONEY/usaedition/2014-12-02-QampA-with-Stephen-Hawking_ST_U.htm.

Tai, Zixue. *The Internet in China: Cyberspace and Civil Society*. 1st ed. Routledge Studies in New Media and Cyberculture. New York: Routledge, 2006.

The Department of Justice. “Congress Explains the USA PATRIOT Act.” *Justice.gov*. Accessed April 21, 2016. https://www.justice.gov/archive/ll/subs/q_support.htm.

Vuori, Juha A. “Illocutionary Logic and Strands of Securitization: Applying the Theory of Securitization to the Study of Non-Democratic Political Orders.” *European Journal of International Relations* 14, no. 1 (March 1, 2008): 65–99.

Wasserstrom, Jeffrey N. *China in the 21st Century: What Everyone Needs to Know*. What Everyone Needs to Know. New York, USA: Oxford University Press, 2010.

Wilkinson, Claire. “The Copenhagen School on Tour in Kyrgyzstan: Is Securitization Theory Useable Outside Europe?” *Security Dialogue* 38, no. 1 (March 1, 2007): 5–25.

Williams, Michael C. “Words, Images, Enemies: Securitization and International Politics.” *International Studies Quarterly*, 2003.

“List of Chinese Laws.” *Hirchina.org*. Accessed May 29, 2016. http://www.hrichina.org/en/list-chinese-laws.

The USA PATRIOT Act: Preserving Life and Liberty. Washington, DC: The Department of Justice, 2001. Accessed April 21, 2016. https://www.justice.gov/archive/ll/what_is_the_patriot_act.pdf.