Contesting the State Securitization of Cyberspace: The Impact of Alternative Securitizing Actors

By Mariya Georgieva

Submitted to
Central European University
Department of International Relations and European Studies

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

Supervisor: Professor Paul Roe

Word Count: 13,894

Budapest, Hungary
2015

Abstract

The world today is embedded in cyber, and the security of cyberspace is often presented as a matter of national security. In the realm of national security, the state has been the most capable and willing director of security; it has the power to identify threats, exaggerate their significance to its survival, and employ far-reaching countermeasures to protect itself. Nevertheless, individuals are not excluded from the field of security. In light of the recent events exposing the excessive surveillance practices of the United States in the name of security, it is important to revisit our knowledge of how and by whom security is managed in order to assess the extent to which cyberspace allows for non-state/individual actors to affect security.

The aim of this thesis is thus two-fold: first, to examine the applicability of the Copenhagen School's securitization theory in the context of cyberspace in the United States by exploring the discourse of key public policy documents; and second, to evaluate the extent to which non-traditional or alternative securitizing actors can impact the ways in which security is conducted in cyberspace. This research will illustrate the securitizing power of the state by reviewing the hypersecuritization discourse of the United States' cyberspace policies in the post-9/11 context. Finally, by studying the case of Edward Snowden's revelations and Snowden as an individual actor, this analysis will show how and when alternative securitizations are formulated and whether they can influence existing approaches of security in cyberspace as a field previously securitized by the state.

Acknowledgements

I would like to thank my supervisor, Professor Paul Roe, for the continuous support and guidance throughout the research process. Without him, I would still be trapped somewhere in the dark theoretical corners of the Copenhagen School. Many thanks to Zsuzsa Toth and Roumy Ivanova for their patience and expertise in the intricacies of the English language. I would also like to express my gratitude to my fellow classmates and the entire IRES Department for making this amazing year possible.

Finally, to my dear friends, Sabra Harris and Jonathan Brenes Salazar: effortlessly and unwittingly you inspire me every day. Thank you for being in my life.

Table of Contents

Introduction

The possibilities for cyber space are enormous for noble and corrupt aims alike. While 'cyber' usually denotes virtual space, cyber actions can also have tangible, physical effects. Many, if not most, of our daily activities are controlled by computers and computer networks embedded in cyberspace. While we have a choice as to whether to use our mobile phones to stay up to date with the news or to read it instead on paper, inevitably few of us can avoid using facilities or services controlled by computers. Within the last two decades critical national infrastructure or "the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof"[1] has been increasingly controlled by computer systems – assets such as electricity generation, water supply, and telecommunications are accessible through and operational within cyber space. As a result, a state's infrastructure is becoming, or is said to have become, more vulnerable to unconventional attacks such as cyber terrorism.

Some of the recent major cyber attacks that have led to an increased awareness of the cyber threat include the 2007 denial-of-service attacks in Estonia; [2] the 2008 attack against three US oil companies, ExxonMobil, Marathon Oil, and ConocoPhillips, allegedly perpetrated by Chinese hackers who managed to steal data on the location, size, and value of oil deposits all over the world; [3] and the computer worm Stuxnet, often described as the world's first digital weapon, which was designed to disrupt Siemens industrial control systems and affected at least

[1] "What is Critical Infrastructure?" *US Department of Homeland Security*, October 24, 2013, last modified 2015, accessed May 16, 2015, http://www.dhs.gov/what-critical-infrastructure.

[2] Which led to an increased attention to cybersecurity worldwide and resulted in the formation of organizations such as the international military organization Cooperative Cyber Defence Centre of Excellence accredited by NATO and based in Tallinn, Estonia.

[3] Kim Zetter, "Hackers Targeted Oil Companies for Oil-Location Data," *Wired*, January 26, 2010, accessed April 24, 2015, http://www.wired.com/2010/01/hack-for-oil/.

a thousand machines, allegedly interfering with Iranian nuclear infrastructure.[4] In response to the inherent vulnerability of cyberspace and to recent cyber attacks, states have significantly increased their focus on issues of cybersecurity and have demonstrated readiness to broaden their national security strategies to include organized responses to cyber threats.

Given the immense technological developments humanity has experienced in the last few decades, specifically in the area of computer and network science, it is not unlikely that cyber space will be the platform on which most future policy questions, of any political sphere, will be decided. Thus, it is crucial to revisit the concept of security in regards to cyber space and specifically the questions of who can make security claims and introduce countermeasures to threats and what entities or values are to be preserved.

The initial reason that inspired the choice of topic is my observation that the security of cyberspace, which is inhabited and utilized by so many different actors on a daily basis and which began as an open source platform, largely self-regulated, now appears to be increasingly, albeit not necessarily successfully, regulated by states. Nevertheless, individual actors can and do intervene in the process of regulating cyber space. This became evident following Edward Snowden's revelations, which became a major source of resistance towards the security practices of the United State and brought forth public awareness of the controversial trade-off between security and privacy as freedom. As the world is becoming more and more interconnected, both on a personal, human level and in a technological sense, it is important to study how cybersecurity has been articulated so far, by whom, and in the name of what entities or values.

[4] David Albright, Paul Brannan, and Christina Walrond, "Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment," *Institute for Science and International Security*, December 22, 2010, accessed May 1, 2015, http://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/.

The purpose of my thesis is then to attempt to answer the following set of questions: What constitutes security in the context of cyberspace? How does the state ‘speak’ cybersecurity in the post 9/11 world? Who else can (successfully) identify, discuss, and influence security issues? For my theoretical basis, I will use one of the most innovative and impactful chapters of Security Studies, the so-called Copenhagen School and its theory of securitization. The theory was first introduced by international relations theorist Ole Wæver [5] and further expanded upon in the seminal work *Security: A New Framework of Analysis* by Wæver, Barry Buzan, and Jaap de Wilde[6] who define ‘securitization’ as the process by which an issue is presented as a security issue that poses an existential threat to a given referent object and requires emergency protection measures[7]. This theory has been applied to a variety of issues ranging from the classical military (war and conflict) to the environmental (climate change) and the societal (migration and refugees) realms. I believe it is particularly suitable to explain the emergence of cyberspace as a security issue and to provide a useful theoretical framework for evaluating non-state security actors, particularly the case of Edward Snowden’s revelations.

The structure of the thesis is as follows: the first chapter provides an extensive overview of the concepts of cyber and cybersecurity in order to shed light on the nature of cyberspace and the reasons why it is a growing topic of concern for national security and a growing topic of interest in security studies. The second chapter explores in depth the securitization theory as formulated by Buzan, Wæver, and De Wilde and elaborated by Hansen and Nissenbaum’s work on discourse; this chapter provides the theoretical

[5] Ole Wæver, “Securitization and Desecuritization,” in Ronnie D. Lipschutz (ed.) *On Security* (New York: Columbia University Press, 1995), 46-86.

[6] Barry Buzan, Ole Wæver, and Jaap De Wilde. *Security: A New Framework for Analysis* (Boulder, CO: Lynne Rienner Pub, 1998).

[7] Ibid., 23-4.

framework needed for analyzing the ways in which the United States has approached issues of cyberspace in the post-9/11 context and for exploring the discourse of securitization in key policy documents. After analyzing the state securitization of cyberspace, the third chapter reviews the language and the impact of Edward Snowden’s revelations in order to examine the impact of securitizing moves performed by non-state actors and to determine the extent to which individuals are able to challenge state securitizations.

1 Cyberspace and Security

This chapter presents an overview of the key concepts used in my thesis: cyber and security. It begins with a review of the existing literature on the concepts of cyber and cyberspace, and proceeds to introduce the concept of security and particularly security of cyberspace.

1.1 The cyber and its embedded insecurity

'Cyber' originates from the Greek adjective *κυβερνητικός* which translates to *skilled in steering or governing* or simply *gubernatorial/governing*.[8] The prefix was first used in the word *cybernetics*, the study of regulatory systems, introduced by MIT Mathematics professor, Norbert Wiener[9]. In its modern use, 'cyber' is attached to words such as space, security, crime, terrorism to connote 'virtual' characteristic. 'Cyberspace' in particular was coined by science fiction author William Gibson in his 1982 book *Neuromancer*, where it is described as "a consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphical representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the non-space of the mind, clusters and constellations of data."[10] Author Michael Heim, whose work explores the philosophy of computing, highlights the intersubjective character of cyber by describing it as a "represented or artificial world, a world made up of the information that our systems produce and that we

[8] Henry G. Liddell and Robert Scott, *A Lexicon Abridged from Liddell and Scott's Greek-English Lexicon* (Clarendon Press, 1869), 384, accessed April 30, 2015, https://books.google.hu/books?id=_40UAAAAYAAJ&dq=liddell+scott+book+greek&source=gbs_navlinks_s.

[9] Norbert Wiener, *Cybernetics, or Control of Communications in the Animal and the Machine* (Cambridge: MIT Press, 1948).

[10] William Gibson, *Neuromancer* (New York: Berkley Publishing Group, 1989), 128.

feed back into the system."[11] While heavily infused with metaphors and other figures of speech, these two descriptions coincide with what we usually tend to understand cyberspace to mean: a network of computers accessed by users. With the advent of the Internet, cyberspace began to be used to refer to the virtual space where online interaction between people takes place. Hence, it is important to stress that in addition to computers, cyberspace today consists of all information and communication technologies (ICTs), including the Internet, emails, television, and mobile phones. Cyberspace encompasses both tangible elements (the hardware and ICTs) and intangible elements (the virtual network between physical components, the software that makes the hardware operational, and the information that is shared).

Nevertheless, the Internet contributed greatly to the all-pervading nature of cyberspace. The Internet was not created with the idea or the expectation for its becoming what it is today, a system of global elaborate interconnectedness. It was born in 1969 as an inter-university project named the Advanced Research Project Agency Network (ARPANET), connecting Stanford, Berkeley, and MIT. Similar projects existed on other campuses in the US and the UK, but this one was the first to implement standardized rules on how data should be transmitted between computers, the so called TCP/IP (Transmission Control Protocol and Internet Protocols),[12] which made communication between different networks possible and which form the backbone of today's Internet. As a result, cyberspace is open to anybody who has access to the Internet. Benevolent and malevolent actors alike

[11] Michael Heim, *The Metaphysics of Virtual Reality* (New York: Oxford University Press, 1993), 78. For more on the early linguistic and philosophical approaches to cyber, see Anna Cigognani, "On the Linguistic Nature of Cyberspace and Virtual Communities," *Virtual Reality* Vol.3, No.1 (1998): 16-24; Michael Benedikt, *Cyberspace: First Steps* (Cambridge: MIT Press, 1991; and Howard Rheingold, *Virtual Communities* (Cambridge: MIT Press, 1993).

[12] Marc Weber, "Who Invented Which Internet?," *Computer History Museum*, September 12, 2012, accessed April 30, 2015, http://www.computerhistory.org/atchm/who-invented-which-internet/.

can use it as a tool to achieve particular goals. Cyberspace's permeability and the increased dependence of a state's critical national infrastructure and services on computer networks have been the source of rising concerns about cyber threats. As early as 1991, a report by the US National Academy of Sciences ominously warned that "tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb."[13]This is why the prefix cyber- has been effortlessly attached to words with negative connotations such as weapons, hate, bullying, and crime, as well as to words describing serious acts of violence such as terrorism and warfare.

Furthermore, the enormous capacity of cyberspace to transmit information and to serve as an access point to various networks has not gone unnoticed by intelligence and military actors. Not surprisingly then cyberspace has been of immense interest to the military. In fact, cyberspace is often called the fifth domain of military operations: "Although it is a man-made domain, cyberspace is now as relevant a domain for DoD activities as the naturally occurring domains of land, sea, air, and space."[14] It is also referred to as an "embedded"[15] domain, because military operations on land, sea, air, and space are all increasingly dependent on cyber operations. Author and senior analyst at the Research ANd Development Corporation (RAND) Bruce Berkowitz further argues that the Information Revolution was the most transformative event for the development and growth of military

[13] National Academy of Sciences (NAS), Computer Science and Telecommunications Board, *Computers at risk: Safe computing in the information age* (Washington, DC: The National Academies Press, 1991), 7.
[14] US Department of Defense*,* "Strategy for Operating in Cyberspace," July 2011, 5, accessed May 15, 2015, www.defense.gov/news/d20110714cyber.pdf.
[15] Gen. Larry D. Welch USAF (Ret.), "Cyberspace – The Fifth Operation Domain," *IDA Research Notes*, Summer 2011, accessed May 15, 2015, https://www.ida.org/~/media/Corporate/Files/Publications/ResearchNotes/RN2011/2011%20Cyberspace%20-%20The%20Fifth%20Operational%20Domain.pdf.

power in the 20th century. [16] From a military perspective, cyber features such as the World Wide Web have created an environment of asymmetrical threat as they allow a weaker actor to breach a more advanced opponent's system and remain unnoticed.

Furthermore, the interconnectedness between cyberspace and physical space is also of concern, because in the complex network of infrastructure and ICTs, cyber actions can have potentially damaging physical effects. The US government reflects these concerns in their strategic plan on the protection of critical infrastructure which elaborates on the importance of securing all infrastructures against all types of risk, including cyber attacks; for this purpose, the Office of Infrastructure Protection actively collaborates with the Office of Cybersecurity & Cyber Communications in order to "better analyze and understand the impacts on physical infrastructure from cyber and control system exploits and develop enhanced risk management solutions".[17] Hence, cyberspace appears to be, by default, insecure, and it is essential for the state that it be secure(d) immediately.

1.2 Cybersecurity

The nature and implications of cyberspace became even more central to state security after the events of 9/11, since the Global War on Terror has sought to establish terrorism in all its forms as the number one security threat and has legitimized the transgression of a range of civil and human rights in the name of national security, such increased surveillance, Guantanamo, and the practice of rendition. The GWoT has also led to increased political engagement with questions of cyberspace in regards to security policies, and many states and international organizations have introduced or revised their policies on cybersecurity. For

[16] Bruce D. Berkowitz, *The New Face Of War: How War Will Be Fought in the 21st Century* (New York: The Free Press, 2003), 3.

[17] US Department of Homeland Security, "Office of Infrastructure Protection Strategic Plan: 2012–2016," *National Protection and Programs Directorate*, August 2012, accessed May 16, 2015, 8, http://www.dhs.gov/office-infrastructure-protection.

example, according to the European Commission, cybersecurity encompasses "the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure" and aims to "preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein."[18] In a similar language, the US Homeland Security website stresses the need for cybersecurity and the resilience of cyberspace against the "increased risk for wide scale or high-consequence events that could cause harm or disrupt services upon which our economy and the daily lives of millions of Americans depend."[19] In response to political statements and public concerns with the vulnerabilities of cyberspace, a number of researchers have focused on cybersecurity as a policy problem and have attempted to solve it through policy suggestions, all the while fully staying within the official discourse of cyber as threatened.[20] Ronald Deibert's work, for example, focuses on analyzing cyber espionage and proposes a comprehensive approach to cybersecurity based on existing democratic traditions[21], while Internet security expert Dan Verton advises the US on how to prepare against cyber terrorism. [22]

Nevertheless, the concepts of cyberspace and cyber threat are elusive and ambiguous. Actual existing threats are hard to pinpoint in a cyber setting, but states do not appear to be

[18] "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace," *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*, (Brussels, February 7, 2013): 3.
[19] "Cybersecurity Overview," *US Department of Homeland Security,* April 27, 2015, accessed May 1, 2015, http://www.dhs.gov/cybersecurity-overview.
[20] Alberts & Papp, 1997; Arquilla, & Ronfeldt, 1993, 1996, 1997, 2001; Deibert, 2000; Molander & Wilson, 1996; Schwartau, 1994; Verton, 2003.
[21] Ronald Deibert, "Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace," *Canadian Defence & Foreign Affairs Institute*, August, 2012, accessed May 15, 2015 http://deibert.citizenlab.org/2012/08/distributed-security-as-cyber-strategy/.
[22] Dan Verton, *Black Ice: The Invisible Threat of Cyber-terrorism* (McGraw-Hill Osborne Media, 2003).

waiting for a real attack to take place in order to prepare a security response. Hence, the traditional (realist/neo-realist) approach of security based on an objectively existing threat falls short of justifying why cyberspace is classified as a security issue in the first place. Furthermore, the policy-driven approach is by default in tune with the assumption that a threat does exist, and so it remains largely uncritical or uninterested in how threats in cyberspace are perceived and constructed by the state.

In contrast, scholars such as Myriam Dunn Cavelty, Lene Hansen, and Helen Nissenbaum observe how, when, and why issues related to cyberspace come to pose a security threat to the state. For example, Cavelty argues that while cyber threats have not actually fully materialized, they have been consistently framed as a grave danger to national security in the terrorism discourse. She also identifies different ways of framing cyber threats as a security problem and analyzes the reasons why cybersecurity has enjoyed such a prominent spot in the US political agenda.[23] The nature of cyberspace as viewed by policy makers in the aftermath of 9/11 seamlessly links the concepts of terrorism and technology, both of which are by default unpredictable and thus, dangerous: “they are ultimately seen as a threat to society’s core values, especially national security, and to the economic and social well-being of a nation” and as a result, cyber threats are “inevitably presented as a national security issue.”[24]

Authors Lene Hansen and Helen Nissenbaum explore further how cyberspace is securitized, or becomes a concern for national security, by utilizing three different grammars or forms of discourse of securitization articulated by the state in reference to cyberspace:

[23] Mary Dunn Cavelty, “Cyber-Terror–Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate,” *Journal of Information Technology & Politics*, 4.1 (2007): 19-36, http://dx.doi.org/10.1300/J516v04n01_03.
[24] Ibid.: 29

‘hypersecuritization’, an exaggeration of the cyber threat and the necessary countermeasures, ‘everyday security practices’, the linking of the threat to citizens’ everyday life, and ‘technification’, the constructing of the cyber threat as a complex issue requiring expert knowledge.[25] These discourses are then observed in the case of Estonia’s responses to the cyber attacks that took place against public and commercial agencies in 2007. By studying these three models of securitization, Hansen and Nissenbaum provide a useful framework for analyzing security as a process constructed and controlled by the state, and one that can be easily observed in other states’ reactions to cyber threats. Furthermore, they introduce another interesting point that has so far remained unexplored in security studies: the idea that cybersecurity discourse brings together different referent objects whose relationship affects the ways in which security is ultimately expressed. These “*competing* articulations of *constellations* of referent objects,”[26] such as network, society, and the sovereignty of the state, present cyberspace as a complex and contested platform that can produce diverse formulations of security.

Nevertheless, diverse formulations of security do not necessarily indicate diverse speakers of security; different actors do not possess equal capabilities to articulate security. In fact, the three languages or grammars of securitizations reviewed here and the cybersecurity countermeasures resulting from the Estonia case suggest that the state is the most privileged ‘speaker’ of security. This raises the question of whether and how alternative articulations of cybersecurity not produced by the states can actually occur and make a lasting impact on our understanding of cyberspace. To attempt to answer this question, I will use the securitization theory as the theoretical framework for my thesis. This theory studies

[25] Lene Hansen and Helen Nissenbaum, “Digital Disaster, Cyber Security, and the Copenhagen School,” *International Studies Quarterly* 53, no. 4 (2009): 1155-1175.
[26] Ibid., 1163.

how and when certain issues become security concerns and identifies conditions and characteristics that empower actors to make security claims. The theory also engages with the interplay within and between security constellations consisting of securitizing actors, referent objects, threats, and facilitating conditions/actors. This is particularly useful for discovering alternative securitizations, actors, and referent objects that can affect cybersecurity.

The concept of state securitization will be observed through analyzing key policy documents demonstrating how the US government managed the security of cyberspace in the post-9/11 context. I have chosen the period after the 9/11 attacks, for they are indicative of and have influenced significantly US defense strategies and overall perceptions of security. I will focus on one of the three securitization discourses discussed by Hansen and Nissenbaum, the so-called hypersecuritization, and will analyze how it has been used to elevate cyber threats and legitimize extraordinary responses in cybersecurity policies. Applying the Copenhagen School's understanding of security to the case of cyberspace will illustrate that despite the theory's supposition that non-state actors can securitize, in reality, the state is significantly better suited than any other actor and is able to sustain stable security constellations that very rarely allow for alternative actors to speak security.

Following the empirical assessment of the securitization theory in the historical context of state securitization of cyberspace, I will try to identify cases in which the state securitization is truly contested. To do this, I will study Edward Snowden's revelations as an alternative securitization of cyberspace that is in conflict with the state securitization. I will attempt to present Snowden as an example of a competing (and unforeseen) security actor who has articulated alternative referent objects and who has had a lasting impact on the state approaches to and people's understanding of cybersecurity.

2 The Securitization Theory and the State

> *No other concept in international relations packs the metaphysical punch, nor commands the disciplinary power of "security." In its name, peoples have alienated their fears, rights and powers to gods, emperors, and most recently, sovereign states, all to protect themselves from the vicissitudes of nature--as well as from other gods, emperors, and sovereign states. In its name, weapons of mass destruction have been developed which have transfigured national interest into a security dilemma based on a suicide pact. And, less often noted in international relations, in its name billions have been made and millions killed while scientific knowledge has been furthered and intellectual dissent muted.*[27]

This chapter presents an overview of the securitization theory and the grammars of securitization introduced by Hansen and Nissenbaum, and then applies the theory to the US government's security strategy in regards to cyberspace following the impact of 9/11. In particular, it analyzes how the hypersecuritization discourse has been utilized in key policy documents in order to illustrate the process and language of state securitization of cyberspace and identify conditions that propel successful securitizations. This provides the theoretical platform used in the last chapter to analyze and evaluate Edward Snowden's actions as an example of an alternative securitization of cyberspace.

2.1 How does 'security' happen? The securitization theory

The post-Cold War world demanded an alternative to or an expansion of the state-centered, military understanding of security. This can be observed in the changing field of security studies shaped by a variety of factors including great power politics, technological developments, and major historical events. New approaches such as constructivism, human security, feminism, and poststructuralism have challenged the traditionalist understanding of

[27] James Der Derian, "The Value of Security: Hobbes, Marx, Nietzsche, and Baudrillard," in *On Security*, ed. Ronnie D. Lipschutz (New York: Columbia University Press, 1995), 25.

security[28]. As part of the widening and deepening trend in security studies, Copenhagen School, with Barry Buzan and Ole Wæver at its core, introduced the so-called 'securitization theory', which views security as "the move that takes politics beyond the established rules of the game and frames the issue as either a special kind of politics or as above politics"[29]. Every public issue can be placed along the spectrum of politics, ranging from nonpoliticized, issues not addressed by the state and outside the public sphere of discussion, through politicized, issues that are discussed by state decision-makers and the public, and finally, to securitized, issues defined as existential and urgent, prioritized over other issues, and resolved by experts in an emergency setting, none of which can be contested[30]. Whether the issue is a threat in the literal, objective sense is irrelevant, for "security […] is a self-referential practice". [31] "An issue is defined as a security issue not necessarily because a real threat exists but because the issue is presented as such a threat"[32] by actors who have securitizing power – most often governments, high-ranking politicians, public officials, and other entities/individuals who have significant political leverage. The issue then becomes a matter of security as a result of a deliberate social process, so understanding securitization in itself requires the understanding of the "the power politics of a concept":

> [S]ecuritization studies aims to gain an increasingly precise understanding of who securitizes, on what issues (threats), for whom (referent objects), why, with what results, and, not least, under what conditions (i.e., what explains when securitization is successful).[33]

[28] Barry Buzan and Lene Hansen, *The Evolution of International Security Studies* (Cambridge: Cambridge University Press, 2009), 187-225.
[29] Buzan et al., *Security: A New Framework for Analysis*, 23.
[30] Ibid., 23-4.
[31] Ibid., 24.
[32] ibid., 24.
[33] Ibid., 32.

Hence, securitization takes place in a system of three key elements or units that can be analyzed individually: a securitizing actor (the actor who performs the securitization), referent object (the object that has "a legitimate claim to survival"[34] and in the name of which the securitization is being done), and functional actors (auxiliary actors who influence the process of securitization). Securitization also requires an audience who accepts or rejects the act of securitization – the response of the audience to the securitizing act helps determine whether the act has been successful. Nevertheless, the authors remain rather vague in theorizing and evaluating the role of the audience.[35] Following the logic of securitization, what constitutes the audience depends on the particular situation of securitization, and thus, fixed parameters for evaluating its role should not be expected; still, within the classical securitization theory, the function of the audience remains underspecified; what is stated is that if the audience does not accept the securitizing act, then the attempt at securitization is described as merely a 'securitizing move'[36].

What happens if the audience does not have explicit knowledge of the securitizing act, however? The security speech act, what the Copenhagen School describes as the "utterance" of security words which positions an issue within an extra-political framework of emergency, could be happening alongside other, strategic acts, which are not necessarily vocalized or visible in the public realm; if the audience is thus unaware, then how can it reject securitization? I will later observe this phenomenon in the case of cybersecurity in which public policy documents presenting securitization speech acts mobilized extraordinary institutional responses (strategic acts) that remained hidden to the public. This case will illustrate how the unawareness of the audience can, in a way, constitute acceptance, and thus,

[34] Ibid., 36.
[35] Ibid., 26–33.
[36] Ibid., 25.

securitization can be successful without the audience being entirely conscious of the range of authorized countermeasures.

Yet, threats are not conjured out of thin air. It is important to stress that the securitization theory does not ignore or diminish the role of objective reality or the factuality of a threat against which a securitizing move is initiated. The actual threat helps establish “common structure perception”[37] between the security agent and the audience, which, while not a deciding factor, can facilitate success of any securitization. The interplay between the securitizing actor and the audience will be explored in the next chapter by analyzing the state’s securitizing moves in the context of cyberspace and the US security strategy after 9/11.

Lastly, the Copenhagen School has contributed to our understanding of security by identifying five different ‘sectors’ in which security and securitizations can take place; these include the military/state, political, societal, economic, and environmental sectors. What varies among the different sectors is the understanding of what constitutes a threat, how survival is defined, what actors can and should securitize, and what values are threatened and need to be preserved. Although, the boundaries of these sectors are not clear-cut, there is an expectation that securitizations in the different sectors focus on different constellations of unites and values. Nevertheless, the state is a recurring referent object in different sectors – when applying the securitization theory to cyberspace, it would be possible to see whether the nature of cyber can foster the emergence of other referent objects contending the state’s primacy.

[37] Thierry Balzacq, “The Three Faces of Securitization: Political Agency, Audience and Context,” *European Journal of International Relations* 11, no. 2 (2005): 181, http://ejt.sagepub.com/content/11/2/171.

Since the cybersecurity of essential computer networks has been regulated by military actors or other state apparatus, such as law enforcement, it can be deduced that cyberspace is securitized within the military/state sector. However, given the ambiguous nature of cyber, it is rather difficult to place it squarely within the standard sectors of security. Cyber attacks can blur the distinction between sectors, because they can threaten national infrastructure, social services, military facilities, telecommunications, and other arenas of concern. In a sense, cyberspace could be viewed as an interconnected sector, one that is able to position all other sectors within a network in which threats have increased mobility and speed; or it could be a suprasector, one that has the ability to position cyber threats higher on the existential pyramid of security issues; and finally, it could act as a progressive sector that is accessible for anyone with a keyboard and Internet connection, and could potentially allow for decentralized or alternative securitizations or even desecuritizations.

While Wæver explains that security is always understood as or in relation to national security, as the concept itself always refers to the state,[38] he remains critical of the state as the sole actor responsible for addressing a security issue. Securitization positions a policy issue within a threat-defense framework, in charge of which most often is the state, and that "is not always an improvement"[39]. Desecuritizing or 'normalizing' issues is the morally desirable alternative. Desecuritization is, in a sense, the ethically superior twin of securitization, and it refers to the process by which a previously securitized issue is stripped of its defining urgency and is politicized or brought back to the "ordinary political sphere" and within 'normal' politics, where is can be discussed and debated by the government and the people in a public setting.

[38] Wæver, "Securitization and Desecuritization", 49.
[39] Ibid., p. 47.

The Copenhagen School thus views securitization as something to be minimized or avoided entirely, and desecuritization, as the "optimal long-range option."[40] Security is crucial for the functioning of a political unity, but securitization is not; nor is it inevitable. People should be aware that:

> [A]ny securitization always rests on a political choice. Security can never be based on the objective reference that something is in and of itself a security problem. That quality is always given to it in human communication. And when securitization is seen as a political choice, there is less chance that security gets idealized as the sought for condition, and more chance that the path to desecuritization—taking things back into normal politics—stands out more clearly.[41]

But while the securitization act has its linguistic equivalent, the speech act, a rhetorical tool through which security is articulated, desecuritization does not have a similar standardized tool through which it can become operational; one cannot simply 'speak' desecurity. Nevertheless, there are several ways in which desecuritization can take place, identified by Lene Hansen: change as stabilization, which implies a sort of accommodation and a temporary commitment of competing security actors to de-escalate security approaches; replacement of issues (which could lead to subsequent securitizations, albeit potentially more desirable); rearticulation, the most unattainable form of desecuritization, which requires a fundamental shift in how political societies engage with security (a process of serious transformation which can take place as a result of changed conditions or can be coerced); and finally, silencing, a "normatively and politically problematic" form of desecuritization, as it eliminates a given issue from the security and political discourses

[40] Buzan et al., *Security: A New Framework*, p. 29.

[41] Barry Buzan and Ole Wæver, "Slippery? Contradictory? Sociologically Untenable? The Copenhagen School Replies," *Review of International Studies* 23.2 (April 1997, published online Sep 8, 2000): 246, http://journals.cambridge.org/abstract_S0260210597002416.

altogether, impeding the possibility of ever resolving it.[42] Securitization then has a dual meaning of politicization (bringing up an issue previously neglected by politics) and anti-politicization (completely removing the issue from politics).[43] Similarly, desecuritization can entail normalization or silencing/repression,[44] the latter altogether defeating the original normative goal of desecuritization. Hence, it is important to analyze where the issue on the nonpolitical-political-securitized continuum was before the process of securitization began and to where the securitization act has moved it, in order to determine whether desecuritization is possible and whether it would be beneficial for the restoring of normal politics. There could be cases in which alternative securitizations and not desecuritizations are most well-suited for restoring public debate, which I will try to demonstrate in the following chapter.

The Copenhagen School understands security as a broad field that can be entered by any type of actor and does not exclude anyone "from attempts to articulate alternative interpretations of security."[45] In reality, however, not everyone can be a security actor and not all actors are equal in security. First, the ability to make successful securitizations depends on the position that the actor has within the field of security. The field is structured in such a way that "some actors are placed in positions of power by virtue of being generally accepted voices of security"[46]. As the "largest universal-purpose collective-action unit,"[47] the state is well-placed to represent important collectivities (i.e. nation, citizens, for example)

[42] Lene Hansen, "Reconstructing Desecuritization: the Normative-Political in the Copenhagen School and Directions for How to Apply it," *Review of International Studies* 38.3 (2012): 538-46, http://dx.doi.org/10.1017/S0260210511000581.
[43] Buzan et al., *Security: A New Framework*, 29.
[44] Buzan and Hansen, *Evolution*, 217.
[45] Buzan et al., *Security: A New Framework*, 31.
[46] Ibid., 31.
[47] Olav F. Knudsen, "Post-Copenhagen Security Studies: Desecuritizing Securitization," *Security Dialogue* 32.3 no.3 (2001): 363.

and make claims on their behalf, and as such, it remains the most prominent and privileged securitization actor.

Moreover, even though the securitization theory stresses that official authority is not necessary to speak security, the official status of the state ensures that it possesses a combination of credibility and expert/technical knowledge unmatched by non-state actors. This will become evident in the case of cybersecurity, as cyberspace is an extremely technical field. In addition to speaking the technical language and other "particular dialects of different sectors",[48] the state is also fluent in the official language of politics and policy-making, something which is not explicitly addressed by the securitization theory – when the state speaks security, it can easily mobilize action (such as policy changes or new laws, for example) in, arguably, a much larger capacity than any other political actor. Finally, being a well-organized system itself with numerous bureaucracies and institutions, the state is well-equipped to navigate, integrate, and regulate other systems, including cyberspace, which is, by nature, an amalgam of systems.

Thus, exploring how the state has securitized cyberspace so far and what characteristics have made it a successful securitizing actor will allow me to assess the possibility and success of alternative, non-state actors who speak security in cyberspace. In order to do this, I will first study the discourse of securitization used in policy documents. In the context of cyberspace, information on actual cyber attacks is most often a matter of national security and thus, largely classified, so quantitative analysis of security is neither a useful nor a truly possible choice of method. As securitization entails performative (simultaneously describing and shaping reality) language through the use of speech acts, the most suitable way of analyzing it is not through specific indicators but through studying its

[48] Buzan et al., *Security: A New Framework,* 313.

discourse. Furthermore, this method of research has been endorsed by the ‘fathers’ of securitization themselves, Barry Buzan, Ole Wæver, and Jaap de Wilde. As they explain, “Whenever discourse and the structures thereof are interesting in themselves, discourse analysis makes sense […] The rhetoric is simple: Read, looking for arguments that take the rhetorical and logical form defined here as security.”[49]

While the focus is on the use of language, it is important to stress that discourse analysis does not study only words or ideas; it “incorporates material as well as ideational factors.”[50] Hence, studying the discourse of the securitization of cyberspace also requires an engagement with the historical context to see how it has contributed to the impact of cybersecurity articulations. Finally, discourse analysis is suitable for cases in which the researcher predicts or believes that discourse itself is powerful enough to influence policy (e.g., security), which is why I agree with Buzan, Wæver, and Hansen that this method is particularly useful for studying securitizations.

2.2 Securitizing language: The securitization of cyberspace after 9/11

The Copenhagen School identifies two categories of facilitating conditions for any securitization: the internal (linguistic-grammatical) and the external (contextual and social).[51] The former refers to the set of procedures which the securitizing actor must follow and the specific language he has to use, while the latter refers to the social or political status from which the actor speaks security. In order to review how the linguistic-grammatical condition is fulfilled in the US government’s securitization of cyberspace, I will use Hansen and Nissenbaum’s theoretical framework of grammars of securitization (hypersecuritization, everyday security practices, and technification) which I believe is a particularly useful

[49] Buzan et al., *Security: A New Framework*, 177.
[50] Lene Hansen, *Security as Practice: Discourse Analysis and the Bosnian War* (New York: Routledge, 2006), 15.
[51] Buzan et al., *Security: A New Framework*, 32.

operationalization for studying discourse as it was designed specifically for the cyber sector.[52] I will focus on the grammar of hypersecuritization as I believe it best demonstrates the urgency that surrounds perceptions of cyber threats and the mobilization that follows the securitization of cyberspace. I have selected to explore the securitization theory in the case of the US because it is one of the leading countries in terms of economy and military spending and as such, is particularly privileged to "talk" and be "heard" on the topic of security.

Furthermore, in order to analyze discourses of securitization, "one does not need to read everything, particularly not obscure texts".[53] Since the process of securitization links political power and language, primary documents such as key policy publications issued by heads of states provide the most useful sources for discourse analysis, as they present the official rhetoric of the securitizing actors, are clearly articulated, and are generally accessible and known to the audience. Also, public policy documents are useful for studying the securitizations discourse because they provide a description of a problem and propose solutions based on technical or professional knowledge – they simultaneously persuade the audience that a problem exits and respond to that problem. In the Copenhagen School's theoretical framework, policy documents can be interpreted as both a move to securitize and a proof of the beginning of a successful securitization, as any issue that warrants its own policy document has already achieved a higher political status.

Hence, the two texts that I will look at are among the most important US documents on cybersecurity strategy in the post-9/11 period: *The National Strategy to Secure Cyberspace of 2003* and the *International Strategy for Cyberspace* of 2011. These are two key White House reports that demonstrate both the power and status of the US government

[52] Hansen and Nissenbaum, "Digital Disaster," 1163.
[53] Buzan et al., *Security: A New Framework*, 177.

as a securitizing actor and the proper grammar of a securitizing speech act in the specific context of cybersecurity. Even though there are certainly other sources that more readily reveal the proper linguistic norm of securitization, such as the US Patriot Act and presidential speeches on terrorist threats, I have chosen to focus on these two strategies because they specifically discuss cyberspace and because they have resulted in major policy and institutional changes.

The National Strategy to Secure Cyberspace of 2003 was introduced with the broad aim of encouraging a variety of entities, such as federal and local state agencies, private companies, and individuals, to access their vulnerabilities to cyber-attacks and take appropriate countermeasures. The text also lists five "national priorities" to provide an initial framework for effective cybersecurity practices focusing on awareness, system security, threat reduction, response, and national and international cooperation.[54] The *International Strategy for Cyberspace* issued in 2011, as the name suggests, is a document that outlines five principles that all states should follow as well as policy suggestions on topics such as cyber defense, law enforcement, international development, and Internet freedom as part of the overall US international cybersecurity agenda.[55] The strategy also stresses the importance of limiting terrorists' abilities to use the Internet for "operational planning, financing, or attacks."[56]

[54] Executive Office of the President of the U.S., *The National Strategy to Secure Cyberspace* (2003), 2-4, https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf.

[55] Executive Office of the President of the U.S., *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (2011), https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

[56] Ibid., 20.

Elements of the hypersecuritization discourse can be easily found in both documents. For example, derivatives of “destroy”, “disrupt”, and “damage” are used numerous times[57] to describe what cyber attackers are capable of doing to critical national infrastructure. Both documents stress the fact that cyber attacks can have a cascading or domino effect: while they may begin in the cyber realm, they can easily cascade across several sectors of critical infrastructure and simultaneously disrupt multiple targets crucial for the functioning of the state. It is absolutely imperative to act, because “[c]yber attacks can burst onto the Nation’s networks with little or no warning and spread so fast that many victims never have a chance to hear the alarms.”[58] In addition to exaggerating the destructive capabilities of cyber attackers, the use of these and similar words also accentuates the vulnerabilities of the referent object: the US is a “nation now fully dependent on cyberspace” and open to exploitation by “anyone, anywhere, with sufficient capability”[59], as actions in cyberspace can “even endanger international peace and security”.[60]

It is also important to note how often cyber attacks are described as “organized” and “sophisticated”.[61] The two policy documents seem to assume that first, there is an adversary to whom attacks can be attributed, and second, that this adversary is capable and willing to take “intrusive” or “malicious”[62] actions against critical infrastructure and by extension, against American society, economy, or national security. This demonstrates the general tendency in any process of securitization to conceive or imagine the opponent as acting in

[57] *National Strategy,* viii, 6, 22, 30, 31, 33, 40; *International Strategy*, 3, 4, 5, 7, 9, 10, 12, 13, 19, 20.

[58] *National Strategy*, 7.

[59] *National Strategy*, 5, 7.

[60] *International Strategy,* 4.

[61] *National Strategy,* viii, ix, xi, 3, 6, 19, 24, 40; *International Strategy,* 8. 13, 20.

[62] *National Strategy*, 8, 22, 29, 37, 47, 50; *International Strategy,* 3, 12, 19, 21, 24.

unity and with intent: one is likely to "actorize" the other side "as a willful chooser rather than a chain in series of events."[63]

Hansen and Nissenbaum make the important point that even though the hypersecuritization discourse seems to rely disproportionally on the future by referring to threats that have not actually materialized yet, it invokes the possibility of what *could* happen if cyberspace is not secured; the risk is too grave and imminent not to be securitized.[64] This is also evident in the discussed documents: the *International Strategy for Cyberspace* dedicates an entire section to "Cyberspace's Future", and many of the proposed policies in both texts stress the need to deter would-be or potential attackers and future cyber threats. [65] Both documents present as a fact the idea that the cyber threat is constantly growing and that rival states and non-state actors such as terrorist organizations are continuously enhancing their capabilities for cyber attacks – the fact that no cyber apocalypse has taken place yet only suggests that would-be attackers are taking their time to better prepare for launching operations.

Another aspect of hypersecuritization that can be found in the two policy documents is the use of military terms and concepts. For example, "defense", "mission", "aggression", "hostile", and "operation"[66] are often used to characterize the necessary responses to cyber threats. This evokes references to and associations with war, a situation in which the only way to preserve the proverbial Self is to destroy the Other and in which the fear of fatality and total destruction legitimizes all and any countermeasures. Thus, the military sub-discourse within hypersecuritization helps overstate the potential impact of cyber threats and

[63] Buzan et al., *Security*, 44.
[64] Hansen and Nissenbaum, *Digital Disaster*, 1164.
[65] *International Strategy*, 7-15 and 13; *National Strategy*, 3, 15, 33.
[66] *National Strategy*, ix, 2, 3, 5, 6, 7, 8, 13, 14, 20, 21, 24, 45, 51 *International Strategy*, 4, 7, 8, 9, 10, 11, 12, 14, 15, 19, 20, 21.

legitimize the need for major countermeasures. It also highlights the overlapping of the securitizing actor and the referent object in the particular context of cyberspace securitization by repeated references to national security and by presenting cyber as embedded in every area or aspect of life. Critical infrastructure might be most susceptible to cyber attacks, but the broad applicability and utility of cyber systems create a referent collectivity or constellation encompassing interlinked concepts such as economy, society, politics, military, environment, and computer networks, rather than just a single referent object. The elements of this referent constellation together are crucial for the survival of the state and each of them is often regulated or at least overseen by the state.

Moreover, in the securitization framework, any area that requires protection will also require tight regulation. By identifying this referent constellation as vulnerable, the state reinforces its position as the best-suited actor to provide security for any element of the collectivity, i.e. any area that uses cyberspace. Hence, through these public policy documents, the US government established itself as the referent supra-unit: it "speaks" security in order to legitimize extraordinary measures to preserve itself in light of existential cyber threats to its stability. Inaction in the face of looming threats to any of the components of the referent constellation could cause the demise of the state and is thus, inconceivable. Therefore, the language of securitization embedded in the two documents demonstrates how the concept of cybersecurity effortlessly links the security of computers or computer networks to that of the state and illustrates the privileged status of the state within the securitization framework as simultaneously the most capable securitizing actor and the most important referent object that needs to be preserved in case of imminent cyber threat.

2.3 Securitizing power and context

In addition to following the linguistic rules of securitization, the securitizing actor also needs to fulfill the external, contextual and social, condition: i.e., he needs to hold a particularly high position in society from which to generate security articulations that carry serious weight and can mobilize policy responses. As Buzan et al explain, the field of security is "structured or biased"[67] and benefits those who are already in power; hence, the state and officials vested with governing power are better placed to articulate successful security speech acts. Given that the two documents in question were published by the White House's Executive Office of the President, they are an extension of the president himself who certainly fulfills the external condition – the president of the US, together only with heads of major defense agencies such as the CIA, has unparalleled capability to execute security speech acts in front of the American nation and the entire world, and thus, undeniably has significant securitizing power.

Here, it is important to note that both texts begin with messages from the respective presidents of the time, Bush and Obama, both of whom quickly establish cyberspace as a problematic area needing immediate solutions. For example, Bush urges the entire American society to "act to reduce our vulnerabilities to these threats before they can be exploited to damage the cyber systems supporting our Nation's critical infrastructures"[68]. Similarly but in a softer language, Obama urges that "we can come together to preserve the character of cyberspace and reduce the threats we face."[69] The two presidents share the belief that cyberspace is a valuable frontier under threat and requires immediate protection, a belief

[67] Buzan et al., *Security: A New Framework*, 31.
[68] *National Strategy*, iii.
[69] *International Strategy*, iii.

made particularly salient because of the two speakers' political status: any actor would be hard-pressed to openly question or oppose it.

Besides the formal capacity to articulate security issues, the president and the White House also have unprecedented credibility, another characteristic that is of crucial importance for the success of any securitizing move. The American people and the world are aware that the White House has almost unlimited access to all kinds of information, including the classified kind. The fact that the securitizing actor and the referent object overlap in this particular securitization of cyberspace further helps the actor's credibility; the Executive Office of the President, representing the US government, is simultaneously the securitizing actor (or better yet, the securitizing collectivity) and the referent object, so it makes sense that it has objective knowledge of its nature and of what threatens it. This credibility, coupled with the capacity of the White House to filter and frame the information it chooses to share with the public, contributes significantly to its securitizing power.

Hence, the securitization of cyberspace by the state followed the two main conditions for success set by the Copenhagen School: the internal, linguistic/grammatical, and the external, contextual/social. By presenting cyberspace through the grammar of hypersecuritization, the state has followed the proper language of security, 'speaking' about cybersecurity in a way that has elevated its importance for the order and stability of the United States. When an issue is presented as a security issue, it is cemented as an objectivity, as something that exists in actuality and requires immediate countermeasures. As Hansen explains, security issues have "political saliency: not only will they be the subject of intense policy activity, they will also be favorably treated when resources are allocated."[70] Hence, it is not surprising that the two discussed documents and the numerous presidential speeches

[70] Hansen, *Security as Practice*, 31.

stressing the vulnerabilities of cyberspace have helped legitimize a series of extraordinary policy measures in the strategic shift towards the militarization of cyberspace. The creation of entities such as the US Cyber Command which has army, navy, marine, and air force components demonstrates the extent to which the securitization of cyberspace has validated the assumption that the domain needs a serious military presence to be secure.

However, following the rules of the threat-discourse-action framework and the articulation of a speech act by a credible actor is not enough for a securitization to be successful. The social interactions between the speaker and the audience also influence when and how security is conjured; to determine the nature of these interactions one needs to be familiar with the time and place in which they happen. For this reason, it is important to discuss the historical context of the post-9/11 era as the key facilitating condition for the securitization of cyberspace. 9/11 was a central event for the reformulation of US security strategy, as it ended a period of "threat deficit" that ensued with the end of the Cold War, a conflict which "for more than 40 years created a common cause and a shared framing that underpinned US leadership in the West."[71]

The tragedy of 9/11, albeit local, was broadcast to the world via print media, television, online news sites, and social media, fostering a new understanding of security in which anyone anywhere is a potential target and exacerbating concerns with the vulnerabilities of all security sectors in the US and the world; it also directly influenced the US government's already expanding security strategy to include major policies on cybersecurity. The repetition of violent images of the twin towers, collapsing again and again, extended the reach of global terror far beyond the virtual space and caused real fear

[71] Barry Buzan, "Will the 'Global War on Terrorism' be the New Cold War?," *International Affairs* 82. No.6 (November 2006): 1101.

even in places that had never experienced terrorism directly. In this context, the 9/11 terrorism discourse of state officials was influenced and was in turn able to influence threat perceptions by exaggerating and linking what could otherwise be sporadic episodes of political violence to cyber attacks taking place in different parts of the world. In this context, exceptional circumstances that usually allow a securitizing actor to raise an issue above normal politics seem to be constantly present.

Hence, the events of 9/11 created an environment of paranoia in which both the securitizing actor and the audience feared the potential catastrophic effects of terrorists employing all possible tools to attack, including new technology. In this historical context, there is no need for an actual precedent of cyber disasters – political officials can evoke the disaster of 9/11 again and again, each time automatically establishing the referent object(s), an embedded collectivity of people, economy, government, and networks, as vulnerable. This in turn has facilitated the securitizations of otherwise non-traditional sectors in need of security, of which cyberspace is an example – just like the US government was able to take extraordinary measures in response to the 9/11 terrorist attacks, so too should it be able to do the same in cyberspace. Referring to past events to stress future possibility of disasters also helps legitimize preventive and even pre-emptive actions. The following paragraph in *The National Strategy* aptly summarizes the process of securitization starting from the conjuring of a painful collective past and identifying the present, existential threat to the accentuating of the vulnerabilities of the referent object and the overstating of the urgent need for extraordinary countermeasures:

> Until recently overseas terrorist networks had caused limited damage in the United States. On September 11, 2001, that quickly changed. One estimate places the increase in cost to our economy from attacks to U.S. information systems at 400 percent over four years. While those losses remain relatively limited, that too could change abruptly. Every day in the United States individual companies, and home computer users, suffer damage from cyber attacks that, to the victims, represent significant losses. Conditions likewise exist for relative measures of damage to occur on a national level, affecting the networks and systems on which the Nation depends.[72]

In addition to evoking collective memory to construct future threats, the congruity with which terrorism and cyberspace are so often linked can also be observed in the way the two concepts are described: both terror and cyber are often portrayed as random, uncontrollable and evading attribution, as frontiers that can produce or foster such massive chaos that they must be controlled and contained at all costs. While 9/11 has helped elevate the word "terrorism" to the status of a universal symbol of catastrophe (simply uttering the word can produce fear and panic even when no attack or threat exists), "cyber" has acquired this status by being discursively linked to malicious actors such as terrorists. For example, even though the two discussed documents aim to establish a cybersecurity strategy, each mentions derivatives of "terrorism" numerous times[73] and expresses the anxiety that if cyberspace is not reigned by the state, then it might end up under terrorist control.

The references to terrorism in the discussed policy documents can also be examples of hypersecuritization discourse, as they dramatize the capabilities and impact of terrorist attacks in cyberspace. Such references then follow both the grammar rules of successful speech acts, as they stress the looming prospect of terrorists affecting any human life and/or everyday activities at any moment through cyberspace; and they also demonstrate how securitizing actors can enhance their status and power by establishing and strengthening the link between terrorism and cyberspace in their speech acts. Therefore, it appears that the

[72] *National Strategy*, 10.

[73] *National Strategy*, viii, 5, 10, 27, 29, 49; 50, 59; *International Strategy*, 5, 12, 20.

Executive Office of the President utilized its inherent securitizing power, followed the linguistic-grammatical rules of speech acts, and took advantage of the historical context to elevate issues of cybersecurity above normal politics and pave the way for extraordinary policy responses. While some of these policy responses were publicly visible in the formation of new institutions, particularly those in charge of military and government cyber security such as the US Cyber Command, the National Cyber Security Division, and the National Cybersecurity and Communications Integration Center, the most extraordinary ones, those regulating commercial use and even private/personal use of cyberspace, took place clandestinely.

3 Snowden's Revelations: An Alternative Securitization

> *For me, in terms of personal satisfaction, the mission's already accomplished. I already won. As soon as the journalists were able to work, everything that I had been trying to do was validated. Because, remember, I didn't want to change society. I wanted to give society a chance to determine if it should change itself.*[74]

This chapter provides an overview of the broad and extraordinary countermeasures taken by the state in response to the perceived cyber threats after 9/11 and particularly those that became evident through Edward Snowden's revelations. It then observes the effects his revelations have had on the state securitization of cyberspace and positions him within the securitization framework as an example of an alternative securitizing actor. The key aim of this chapter is to establish Snowden as a non-state/individual securitizer who was able to challenge the state and who has helped reinstate public debate and scrutiny of previously securitized issues of cyberspace.

3.1 Case study: The language and context of Snowden's revelations

On June 6, 2013, *The Guardian* published a story by journalist Glenn Greenwald commenting on a secret Foreign Intelligence Surveillance Court's order which required Verizon to hand over their users' phone data to the National Security Agency (NSA). In this article, Greenwald elaborated on the type of data that NSA had access to and expressed a serious concern with how NSA "has transformed from an agency exclusively devoted to foreign intelligence gathering, into one that focuses increasingly on domestic

[74] Bridie Jabour, "Edward Snowden Declares 'Mission Accomplished' in Moscow Interview," *The Guardian*, December 24, 2013, accessed June 1, 2015, http://www.theguardian.com/world/2013/dec/24/edward-snowden-i-already-won.

communications."[75] This publication was the first in a series of leaks revealing the sweeping powers of the agency including programs such as PRISM (a downstream engine collecting data directly from Google, Facebook, YouTube, and other corporations), Boundless Informant (a mapping and auditing tool for global surveillance data), and XKeyscore (an elaborate search database filing the online activities of millions of people). These programs were the institutional results of the post-9/11 state securitization of cyberspace, demonstrating that once securitization is accepted by the audience and the issue is moved away from ordinary politics, future extraordinary countermeasures in the securitized field can be taken in total secrecy in a process of "package legitimization"[76], in which there is no need for audience's subsequent approval or even awareness. This also shows how securitization strengthens the status quo, making it extremely difficult for alternative, non-state actors to question or contest the state securitization, as they would first have to be familiar with the countermeasures in order to oppose them meaningfully.

The first several publications did not identify or refer directly to their source of information, but instead simply described the story as "obtained" by *The Guardian*. The source later revealed his identity as 29-year-old former CIA technology specialist and current Booz Allen Hamilton employee and NSA contractor, Edward Snowden, in an interview by Greenwald and filmmaker Laura Poitras. [77] In this interview, Snowden explained his motives and expressed his hope that the revelations will spark a debate on US domestic spying

[75] Glenn Greenwald, "NSA Collecting Phone Records of Millions of Verizon Customers Daily," *The Guardian*, June 6, 2013, accessed May 22, 2015, http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

[76] Buzan et al., *Security: A New Framework*, 28.

[77] Glenn Greenwald and Laura Poitras, "NSA Whistleblower Edward Snowden: 'I Don't Want to Live in a Society That Does These Sort of Things'" (video), *The Guardian*, June 9, 2013, accessed May 23, 2015, http://www.theguardian.com/world/video/2013/jun/09/nsa-whistleblower-edward-snowden-interview-video.

activities and other disturbing intelligence practices. His biggest concern was that the revelations might run their course silently and might not start a public conversation on the NSA's serious abuse of power. In hindsight, Snowden's actions certainly inspired a huge debate and caused the US government to revisit (publicly) several of its cybersecurity policies.

The revelations initiated a major assessment of NSA's surveillance policies, including a 308-page report by the President's Review Group on Intelligence and Communications Technologies convened by the executive branch and consisting of six experts including Richard Clarke, then National Coordinator for Security, Infrastructure, and Counter-terrorism, and Michael Morrell, Deputy Director of CIA. Even though the report did not mention Snowden or his revelations, it made 46 recommendations aimed to protect national security, respect privacy and civil liberties, and reduce "the risk of unauthorized disclosures".[78] Furthermore, Obama announced a series of major reforms to NSA's activities including: changing how it collects phone data, establishing an independent commission to review its surveillance practices, and adding a public advocate to the FISA Court to represent privacy interests.[79] All the while however, he refused to credit Snowden with these policy changes and even claimed that he had called for a review long before the revelations, stating that "we would've gotten to the same place and we would've done so without putting at risk our national security […] My preference would have been for a lawful, ordinary examination

[78] Richard A. Clarke, Michael J. Morell, Geoffrey R. Stone, Cass R. Sunstein, and Peter P. Swire, *Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies*, December 12, 2013, 1, https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

[79] Walter Hickey and Josh Barro, "Obama Slams GOP on Health Care and Immigration, Proposes to Reform PATRIOT Act," *Business Insider*, August 9, 2013, accessed May 30, 2015, http://www.businessinsider.com/live-barack-obama-is-about-to-answer-americas-questions-2013-8.

of these laws, a thoughtful fact-based debate that would then lead us to a better place."[80] Even so, an ordinary examination does not necessarily mean a public debate, and given the fact that the practices in question were happening clandestinely, it is highly unlikely that such a review would have been open to the audience in absence of Snowden's impact.

Snowden is an individual, non-state actor with no (or, at best, limited) political power, no official authority, no institutional back-up, no prior experience in articulating security, and initially, with a rather dubious credibility due to anonymity. Why was he then able to 'speak' security and repoliticize certain cybersecurity issues? To review Snowden's revelations as an example of a securitizing move contesting the state securitization of cyberspace requires analyzing the discourse used in his interviews and the personal and contextual characteristics or conditions that have allowed him to make security claims. A close look at Snowden's first interviews reveals elements from Hansen and Nissenbaum's securitization discourse models, particularly hypersecuritization and technification. Snowden incorporates linguistic elements of hypersecuritization for two key reasons: to establish himself as an actor with security claims and to designate NSA as a security threat. For example, Snowden's descriptions of NSA create a profile of an omniscient, omnipresent, and omnipotent organization – as he explains, the "world's most powerful intelligence agency […] completely free from risk" can not only collect all information existing virtually about you but also trace and access your physical location and imprints at any time.[81] He continuously stresses that these are exceptional and far-reaching abilities, and the fact that they have been exercised in secret makes them even more alarming; "any analyst at any time

[80] The White House, "Remarks by the President in a Press Conference," August 9, 2013, accessed May 30, 2015, https://www.whitehouse.gov/the-press-office/2013/08/09/remarks-president-press-conference.
[81] Greenwald and Poitras, "NSA Whistleblower" (video).

can target anyone"[82] from ordinary people to high political officials without that target's permission or knowledge.

He also stresses the potential ability of the state to recover from the inculpating effect of the revelations by granting itself more power and "greater control" over the American people, emphasizing the state's inherent structural power to securitize and its almost unlimited ability to regulate the security status quo. This is precisely what Snowden is urging people to rise against: allowing the government to gain more, "new and unpredicted" power is extremely dangerous and it would create a cycle of "turnkey tyranny", an elaborate, self-serving system that would progressively become harder to stop. Inaction on the part of the audience would only strengthen the state securitization of cyberspace, further obscuring and distancing issues of cybersecurity from the reach of political, judicial, and public oversight.

The government's immediate response to the revelations was to cast Snowden as a criminal and an enemy. In July, 2013, the US filed espionage and theft charges against him[83] in order to try and strip him of his credibility, contain him within the established system of crime and punishment, and thus, silence his alternative securitizing speech acts. The discourse of terrorism was also used to delegitimize Snowden and those who have assisted him: in *No Place To Hide*, which follows closely Glenn Greenwald's first contact with Snowden, Greenwald recounts how the British authorities detained his partner at Heathrow airport under the antiterrorism statute because they considered the online leaking of the Snowden documents as "designated to influence a government and [is] made for the purposes

[82] Ibid.

[83] "US Files Criminal Charges against NSA Whistleblower Edward Snowmen," *The Guardian*, June 22, 2013, accessed May 30, 2015, http://www.theguardian.com/world/2013/jun/22/us-charging-edward-snowden-with-espionage.

of promoting a political or ideological cause."[84] Here, we observe once again the link between terrorism and cybersecurity threats, which was a facilitating factor for the state securitization of cyberspace, now used to diminish Snowden's securitizing impact.

By describing Snowden as a criminal, a terrorist, or an individual assisting the enemy (China and/or Russia), the government also evoked the friend-enemy framework of hypersecuritization previously used to securitize cyberspace. This did not succeed in nullifying Snowden's credibility, however, because it quickly became evident that Snowden was not aiding enemies and was not acting to preserve his own security, and because he also garnered support among a large audience including foreign officials targeted by NSA's surveillance programs, human rights organizations, and celebrities. In fact, the possibility of facing arrest and serious punishment helped him gain the moral high ground and trustworthiness in the eyes of the public. As he explains, if you were living "in paradise and making a ton of money, what would it take to make you leave everything behind"[85] and endanger your life by disclosing a bulk of classified documents and then revealing your identity? His actions make it clear that his intent is grounded in a moral code in which the values important for the broader public rank higher than his own security. Throughout his interviews, he repeatedly explains how these values, particularly freedom and privacy, are violated by the government's control of cyberspace and stresses that anyone who believes in these values has an obligation to act. Using such elements of the morality discourse is an effective way to frame his message – because morality implies a system of behavior that is not controlled by any particular authority, any actor who can 'speak' morality can be 'heard' when invoking the common good.

[84] Glenn Greenwald, *No Place to Hide* (New York: Metropolitan Books, 2014), 186.
[85] Greenwald and Poitras, "NSA Whistleblower" (video).

Furthermore, the interviews reveal Snowden's vastly different understanding of security compared to the state's understanding. He urges that, "We shouldn't elevate leaders above the average citizen because, really, who is it that they're working for?"[86] National security should not be separate and above public interest. On the contrary, national security *is* the security of all American people, and as such, it should uphold the values of privacy and freedom, not violate them. Cyberspace is thus not to be isolated and fenced by security agencies; rather, it should be open to all subjects of security, including ordinary citizens so that they could then decide how to operate it.[87] Hence, the hypersecuritization grammar in Snowden's interviews demonstrate that the stark, zero-sum divide between national security and civil liberties, which is revealed in the extraordinary way the state handles cybersecurity, ultimately makes the necessary balance between them impossible.

Another discourse of securitization employed by Snowden, technification, can be seen in the way he describes the programs designed by NSA. He constantly refers to technical terms such as "track" and "intercept communication", "collecting systems", "encryption", and "cloud computing". He also warns that NSA can and does "target the communications of everyone [and] ingests them by default, it collects them in a system and it filters them and it analyzes them and it measures them and it stores them for periods of time".[88] Snowden also discusses the distinction between print and digital private data that NSA tries to promote in its securitization discourse. He argues that this distinction is dangerous and artificial and skews the scale in favor of the state by casting the digital as a

[86] Alan Rusbridger and Ewen MacAskill, "Edward Snowden Interview - The Edited Transcript," *The Guardian*, July 18, 2014, accessed May 25, 2015, http://www.theguardian.com/world/2014/jul/18/-sp-edward-snowden-nsa-whistleblower-interview-transcript.

[87] Rusbridger and MacAskill, "Edward Snowden Interview"; Greenwald and Poitras, "NSA whistleblower" (video).

[88] Greenwald and Poitras, "NSA Whistleblower" (video).

complex and technical domain in need of regulation. Thus, it is evident that while the state uses the technification discourse to justify the need to monopolize control over cyberspace, Snowden's purpose here is not to securitize cyberspace because of its perceived technical complexity but to reveal to the audience the immense technical capabilities at the hands of the government.

Hence, the hypersecuritization and the technification discourses illustrate the linguistic competence of certain actors and the hegemonizing power inherent to language – the public's technical illiteracy and asymmetric access to information allows experts and state officials to successfully 'speak' security regardless of whether the speech act is fully comprehended by the public. Sometimes actors can use that competence to their own advantage at the expense of the public good. As Snowden points out in his second interview, NSA and the US government are examples of power structures "working to their own ends to extend their capability at the expense of the freedom of all publics"[89], and this asymmetry between the power of the state and the power of the public must be eliminated.

3.2 The impact of Snowden as an alternative securitizing actor

In addition to analyzing Snowden's discourses of securitization, it is important to identify the external or contextual characteristics that help establish him as a securitizing actor able to challenge the state securitization of cyberspace. While he was not part of the formal state structure designed to articulate securitizing speech acts and enact extraordinary countermeasures, he certainly benefitted from it because that state structure gave him access to classified information. In the interviews, Snowden recognizes his privileged professional status as a technology expert and explains that it provided him with the actual opportunity to

[89] Glenn Greenwald and Laura Poitras, "Edward Snowden: 'The US Government Will Say I Aided Our Enemies'" (video), *The Guardian*, July 8, 2013, accessed May 30, 2015, http://www.theguardian.com/world/video/2013/jul/08/edward-snowden-video-interview.

gain direct access to all the NSA files he later chose to reveal. Furthermore, his social identity as a security analyst also added to his effectiveness as a securitizer by building his reputation as an individual who has technical knowledge of threats and security.

Nevertheless, he was not the only person in such a superior position. As many as five million Americans have some type of security clearance and 500,000 private contractors have top security clearance[90]. This is why, it is important to stress that his capability to undertake acts contesting the state securitization of cyberspace was coupled with the active choice to do so – he talks of feeling “compelled” to take action and explains that the increased “awareness of wrongdoing”[91] had pushed him to act. However, he also views his status as problematic, as it provides him with the power to make decisions that should be reserved for the public instead. The policies guiding state conduct in cyberspace need to be determined by the audience, “not by somebody who is simply hired by the government.”[92] Hence, his revelations are facilitated by his privileged status but also strip him of that status and the rights and responsibilities that come with it; this makes his actions truly an *alternative* securitizing move, as classical securitizations usually increase the securitizer’s rights and powers.

Furthermore, his self-identification as an actor opposing the government is noteworthy, as it demonstrates that the decision to reveal those documents was taken with the full intention to challenge the state’s conduct, to “subvert the government,”[93] as he himself states. This simultaneously actorizes the revelations and presents the government’s

[90] Brett LoGiurato, “How a GED-Holder Managed to Get ‘Top Secret’ Government Clearance,” *Business Insider*, June 10, 2013, accessed May 31, 2015, http://www.businessinsider.com/edward-snowden-top-secret-clearance-nsa-whistleblower-2013-6.
[91] Greenwald and Poitras, “NSA whistleblower” (video).
[92] Ibid.
[93] Ibid.

securitization of cyberspace as a serious event necessitating opposition. Snowden's greatest fear was that nothing would change. Change is thus the ultimate goal of his actions – not just ensuring public awareness but mobilizing counteraction.

Political power in the information age is partially determined by credibility grounded in the capacity to filter, frame, and distribute valuable information to the public.[94] As the state's ability to securitize is partially based on its framing power, it is important to review whether Snowden had framing power and to what extent it has facilitated his alternative securitization of cyberspace. In the interviews, Snowden asserts several times that none of the leaked information has been altered by him, that, in a sense, he has not filtered or framed the message to benefit himself or any other actor but the audience. Nevertheless, his decision to reach out to Greenwald and Poitras for publishing the documents in initial anonymity was very deliberate. Greenwald is an investigative journalist and constitutional lawyer, and Poitras is an Academy-Award winning documentary film director known for her work on uncovering dubious US intelligence practices. These are two people with well-established credibility grounded in their broad access to information and their ability to filter that information and expose governments' misuses of power. By letting these particular individuals decide how to present the information to the public, Snowden has, in an indirect manner, filtered and framed the relevant information for his goal of exposing government misconduct. Outsourcing a part of the framing process to media professionals with already established credibility and social interests is thus an exercise of political power and helps position Snowden as an influential securitizing actor.

[94] Robert O. Keohane and Joseph S. Nye, "Power and Interdependence in the Information Age," *Foreign Affairs* 77, no. 5 (1998): 81-94.

Ultimately, the state's securitizing reasoning is based on the consequential goal of providing security as freedom from cyber threats at all costs. In contrast, Snowden's actions are aimed at restoring the ability of every individual to decide for herself whether and how to participate in the digital world. For this, however, the digital world must be first and foremost open and transparent. Hence, by exposing the full effects of the NSA surveillance practices, Snowden's actions suggest that the state securitization of cyber space has eroded people's trust in their government. The state, not any foreign entity, is the real security threat. In Snowden's securitization framework then, trustworthiness achieved by a free and open digital space with explicitly stated regulatory parameters is a precondition for security, not an effect of it; this is in polar opposition to the government practice of 'collect all' (data) to find the truth.

His revelations then completely reverse the perceived threat – the real danger is not that cyberspace is unpredictable and exploitable by dangerous actors, but that it is being currently exploited by the government in grave abuse of power under the secretive banner of national security. Furthermore, through his alternative speech act following the proper grammars of securitization (i.e. the publication of the leaks), Snowden has successfully challenged the state securitization of cyberspace by introducing a constellation of alternative referent objects in need of protection, including individual security, the broader security of the American people and the world, and values such as privacy and freedom, and by calling for public mobilization against surveillance practices. His revelations have forced NSA to publicly justify its programs and demonstrate whether the balance between the cyber threat and the security countermeasures is actually maintained, and that balance has turned out to be significantly skewed.

In effect, the leaks have seriously undermined the state as a securitizing actor by questioning its intent and showing that the surveillance countermeasures are a greater threat to society than to the cyber threats they were created to combat. By compromising people's private information in the name of national security, NSA actually strips individuals from their agency in the name of state security. Snowden's replacement of threats and the distinction he makes between the security of the *nation*, a concept representing a collectivity of people, and the security of the *state*, an institution failing to represent the people, is made clear in the following excerpt:

> We constantly hear the phrase "national security" but when the state begins… broadly intercepting the communications, seizing the communications by themselves, without any warrant, without any suspicion, without any judicial involvement, without any demonstration of probable cause, are they really protecting national security or are they protecting state security?[95]

It is evident that as a result of the revelations, the state has undergone a complete transformation: from a securitizing actor, an entity privileged with the right to conduct security, to a serious threat to cybersecurity. Snowden's actions have successfully shifted the focus of the securitization of cyberspace from values such as the survival of the state and effective national security to the survival of privacy and personal choice. As every securitizing actor, however, his choice to make the revelations was not devoid of politics. It was, indeed, an alternative exercise in the extreme politics of security, a political decision aimed to contest the state securitization of cyberspace and bring to the attention of the public the state's violation of their rights in order to reestablish public debate and oversight on key security issues.

[95] Rusbridger and MacAskill, "Edward Snowden Interview".

Conclusion

This thesis explored the applicability of the securitization theory in the context of cyberspace through a discourse analysis of two key policy documents and then assessed Edward Snowden as an alternative securitizing actor and explored his impact on the state's approach to cybersecurity. The application of the securitization theory to cybersecurity policy after 9/11 has effectively demonstrated that the state's security conduct is neither inevitable, nor impartial. The ability to identify urgent and grave threats, raise them above politics, and legitimize extraordinary countermeasures belongs to actors who follow the grammar rules of securitization and who hold a position of power granting them credibility. Most often the game of securitization benefits established systems of power: such as the state or individuals who represent the state. On rare occasions, however, alternative individual actors can successfully challenge state securitization, as this thesis showed with the case of Edward Snowden's revelations. By raising awareness to the draconian surveillance measures employed after 9/11, Snowden transformed cyberspace from securitized as a threat by the state to a subject of public debate and resistance. NSA's elaborate tools to track online activity and their use of secret courts to extract user data from private companies revealed by Snowden have created an environment of no incentive for governmental limitation or transparency, an environment in which the individual is a subject of cybersecurity but is neither aware of nor benefiting from that subjectivity.

At the time of writing this conclusion, Section 215 of the US Patriot Act used for NSA's bulk phone and other data collection has just expired.[96] For the first time since 2001, the US government is relinquishing, instead of adding, powers vested in one of the most

[96] Erin Kelly, "Here's What Happens Now That the Patriot Act Provisions Expired," *USA TODAY*, June 1, 2015, accessed June 1, 2015, http://www.usatoday.com/story/news/nation/2015/05/31/patriot-act-expires-senate-stalemate/28260905/.

important key anti-terrorist legislative document. This is a major event that was directly induced by Snowden’s revelations, and it will most likely continue to inspire diverse reactions and heated debates among political leaders and the public. At the same time, the proposed alternative bill under the name USA Freedom Act has been put on hold. The current state of limbo is indicative of the success of Snowden’s revelations; it will be interesting to see whether the Freedom Act is passed, amended, or substituted with a new or reformed bill reminiscent of the Patriot Act, but regardless of the outcome, this event is a clear example of restored public debate and scrutiny on previously secret surveillance programs. Snowden’s actions likely constitute the first step in a long process of challenging the state securitization of cyberspace and establishing the potential for long term desecuritization.

Furthermore, this thesis has demonstrated that Snowden’s revelations are simultaneously performative, as they constitute securitizing moves, and self-reflective; Snowden remains critical of the logic of the state securitization of cyberspace and the measures that he proposes are hardly extraordinary. On the contrary, the measures he calls for involve the normalization or repoliticization of cybersecurity, for they aim to foster public discussion of the ways the state regulates content and use of cyberspace.

The success of a securitizing move is determined by its effects and thus, traditional securitization studies often provide an outcome-centered approach to security and formal political power as structural advantage for securitizing actors. As a result, it is easy to overlook the impact of individuals. Nevertheless, as the case of Snowden’s revelations has shown, individual acts can spark a public debate and result in cumulative effects that are far from insignificant within the securitization frameworks. Security is intersubjective, and

Snowden’s actions have reminded us that we, constituting the audience in the securitizing moves made by the state, are in fact, also subjects in cyberspace and can and should be able to influence or challenge whether and how it is securitized. He did this by using the same linguistic-grammatical models used by the state, particularly hypersecuritization, and he took advantage of his powerful position within the US security institutions. Thus, this thesis has demonstrated that social status and professional background of the individual matter significantly for successful securitizations and can constitute a sort of informal political power: people with experience in the security field are better placed to make securitizing moves than non-security actors.

Edward Snowden’s case is new and its impact is still accumulating, so it allows for original interpretations to be made on the individual actor’s securitizing agency. Still, for reasons of scope and space, this research has only focused on the field of cybersecurity and on one individual actor of securitization. Further empirical analysis of other similar actors such as whistleblowers Julian Assange and Chelsea Manning would considerably expand our understanding of the role of individuals in the framework of securitization and desecuritization. In addition to providing an analysis of the securitization discourse used in policy documents, this thesis has also demonstrated the importance of political and social capital for effective securitization. Snowden’s wide support greatly contributed to his success as a securitizer and so, a further study on the impact of informal (nonpolitical) credibility on securitizing power would enhance our understanding of the external, contextual facilitating conditions of securitization that could potentially allow for other alternative, non-state securitizing actors to emerge.

Bibliography

Albright, David, Paul Brannan, and Christina Walrond. "Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment." *Institute for Science and International Security*. December 22, 2010. Accessed May 1, 2015. http://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/

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

Berkowitz, Bruce D. *The New Face Of War: How War Will Be Fought in the 21st Century*. New York: The Free Press. 2003.

Buzan, Barry and Lene Hansen. *The Evolution of International Security Studies*. Cambridge: Cambridge University Press. 2009.

Buzan, Barry and Ole Wæver. "Slippery? Contradictory? Sociologically Untenable? The Copenhagen School Replies." *Review of International Studies* 23.2. (April 1997, published online Sep 8, 2000): 246. http://journals.cambridge.org/abstract_S0260210597002416.

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

Cavelty, Mary Dunn. "Cyber-Terror–Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate." *Journal of Information Technology & Politics* 4.1 (2007): 19-36. http://dx.doi.org/10.1300/J516v04n01_03.

Clarke, Richard A., Michael J. Morell, Geoffrey R. Stone, Cass R. Sunstein, and Peter P. Swire. *Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies*. December 12, 2013. https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

"Cybersecurity Overview." US Department of Homeland Security. April 27, 2015. Accessed May 1, 2015. http://www.dhs.gov/cybersecurity-overview.

"Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace." *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*. Brussels. February 7, 2013.

Executive Office of the President of the U.S. *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (2011). https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

Executive Office of the President of the U.S. *The National Strategy to Secure Cyberspace* (2003). https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf.

Deibert, Ronald. "Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace." *Canadian Defence & Foreign Affairs Institute*. August, 2012. Accessed May 15, 2015. http://deibert.citizenlab.org/2012/08/distributed-security-as-cyber-strategy/.

Der Derian, James. "The Value of Security: Hobbes, Marx, Nietzsche, and Baudrillard." *In On Security*. Edited by Ronnie D. Lipschutz, 24-45. New York: Columbia University Press, 1995.

Gibson, William. *Neuromancer*. New York: Berkley Publishing Group. 1989.

Greenwald, Glenn. *No Place to Hide*. New York: Metropolitan Books. 2014.

Greenwald, Glenn. "NSA Collecting Phone Records of Millions of Verizon Customers Daily." *The Guardian*. Last modified 2013. Accessed May 22, 2015. http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

Greenwald, Glenn and Laura Poitras. "Edward Snowden: 'The US Government Will Say I Aided Our Enemies.'" Video. *The Guardian*. July 8, 2013. Accessed May 30, 2015. http://www.theguardian.com/world/video/2013/jul/08/edward-snowden-video-interview.

Greenwald, Glenn and Laura Poitras. “NSA Whistleblower Edward Snowden: ‘I Don't Want To Live In A Society That Does These Sort Of Things.’” Video. *The Guardian*. June 9, 2015. Accessed May 23, 2015. http://www.theguardian.com/world/video/2013/jun/09/nsa-whistleblower-edward-snowden-interview-video.

Hansen, Lene. “Reconstructing Desecuritization: the Normative-Political in the Copenhagen School and Directions for How to Apply it,” *Review of International Studies* 38.3 (2012): 538-46. http://dx.doi.org/10.1017/S0260210511000581.

Hansen, Lene. *Security as Practice: Discourse Analysis and the Bosnian War*. New York: Routledge. 2006.

Hansen, Lene and Helen Nissenbaum. “Digital Disaster, Cyber Security, and the Copenhagen School.” *International Studies Quarterly* 53, no. 4 (2009): 1155-175.

Heim, Michael. *The Metaphysics of Virtual Reality*. New York: Oxford University Press, 1993.

Hickey, Walter and Josh Barro. “Obama Slams GOP on Health Care and Immigration, Proposes to Reform PATRIOT Act.” *Business Insider*. August 9, 2013. Accessed May 30, 2015. http://www.businessinsider.com/live-barack-obama-is-about-to-answer-americas-questions-2013-8.

Kelly, Erin. “Here's What Happens Now That the Patriot Act Provisions Expired.” *USA TODAY*. June 1, 2015. Accessed June 1, 2015. http://www.usatoday.com/story/news/nation/2015/05/31/patriot-act-expires-senate-stalemate/28260905/.

Keohane, Robert O., and Joseph S. Nye. “Power and Interdependence in the Information Age.” *Foreign Affairs* 77, no. 5 (1998): 81-94.

Knudsen, Olav F. “Post-Copenhagen Security Studies: Desecuritizing Securitization.” *Security Dialogue* 32.3, no.3 (2001).

Jabour, Bridie. “Edward Snowden Declares ‘Mission Accomplished’ in Moscow Interview.”

The Guardian. December 24, 2013. Accessed June 1, 2015. http://www.theguardian.com/world/2013/dec/24/edward-snowden-i-already-won.

Liddell, Henry George, Robert Scott, and James Morris Whiton. *A Lexicon Abridged From Liddell And Scott's Greek-English Lexicon*. Clarendon Press. 1869.

LoGiurato, Brett. “How A GED-Holder Managed To Get ‘Top Secret’ Government Clearance.” *Business Insider*. June 10, 2013. Accessed May 31, 2015. http://www.businessinsider.com/edward-snowden-top-secret-clearance-nsa-whistleblower-2013-6.

National Academy of Sciences (NAS). Computer Science and Telecommunications Board/ *Computers at risk: Safe computing in the information age*. Washington, DC: The National Academies Press. 1991.

Rusbridger, Alan, and Ewen MacAskill. “Edward Snowden Interview - The Edited Transcript.” *The Guardian*. Last modified 2014. Accessed May 25, 2015. http://www.theguardian.com/world/2014/jul/18/-sp-edward-snowden-nsa-whistleblower-interview-transcript.

US Department of Defense. “Strategy for Operating in Cyberspace.” July 2011. Accessed May 15, 2015. www.defense.gov/news/d20110714cyber.pdf.

US Department of Homeland Security. “Office of Infrastructure Protection Strategic Plan: 2012–2016.” *National Protection and Programs Directorate.* August 2012. Accessed May 16, 2015. http://www.dhs.gov/office-infrastructure-protection.

“US Files Criminal Charges against NSA Whistleblower Edward Snowmen.” *The Guardian*. June 22, 2013. Accessed May 30, 2015. http://www.theguardian.com/world/2013/jun/22/us-charging-edward-snowden-with-espionage.

Verton, Dan. *Black Ice: The Invisible Threat of Cyber-terrorism*. McGraw-Hill Osborne Media. 2003.

The White House. “Remarks by the President in a Press Conference.” August 9, 2013.

Accessed May 30, 2015. https://www.whitehouse.gov/the-press-office/2013/08/09/remarks-president-press-conference.

Wiener, Norbert. *Cybernetics, or Control of Communications in the Animal and the Machine*. Cambridge: MIT Press. 1948.

Wæver, Ole. "Securitization and Desecuritization." In *On Security*, edited by Ronnie D. Lipschutz, 46-86. New York: Columbia University Press. 1995.

Weber, Marc. "Who Invented Which Internet?" *Computer History Museum*. September 12, 2012/ Accessed April 30, 2015. http://www.computerhistory.org/atchm/who-invented-which-internet/.

Welch, Larry D. "Cyberspace – The Fifth Operation Domain." *IDA Research Notes*. Summer 2011. Accessed May 15, 2015. https://www.ida.org/~/media/Corporate/Files/Publications/ResearchNotes/RN2011/2011%20Cyberspace%20-%20The%20Fifth%20Operational%20Domain.pdf.

"What is Critical Infrastructure?" *US Department of Homeland Security*. October 24, 2013. Last modified 2015. Accessed May 16, 2015. http://www.dhs.gov/what-critical-infrastructure.

Wiener, Norbert. *Cybernetics, or Control of Communications in the Animal and the Machine*. Cambridge: MIT Press. 1948.

Williams, Michael. "Words, Images, Enemies: Securitization and International Politics." *International Studies Quarterly* 47, issue 4 (December 2003): 511–531. http://dx.doi.org/10.1046/j.0020-8833.2003.00277.x.

Zetter, Kim. "Hackers Targeted Oil Companies For Oil-Location Data". *Wired*. January 26, 2010. Accessed May 22, 2015. http://www.wired.com/2010/01/hack-for-oil/.