Journal of Research in Applied Linguistics
ISSN: 2345-3303 – E-ISSN: 2588-3887 – https://rals.scu.ac.ir
Published by Shahid Chamran University of Ahvaz

Please cite this paper as follows:

Noori, F., Ameli, S. R., & Hosseini, H. (2024). Elite influence and threat construction by language; The discursive features of the US militarization of cyberspace in Obama administration. *Journal of Research in Applied Linguistics*, *15*(1), 107-127. https://doi.org/10.22055/RALS.2022.39479.2681

Shahid Chamran University of Ahvaz

Research Paper

Elite Influence and Threat Construction by Language: The Discursive Features of the US Militarization of Cyberspace in Obama Administration

Farnaz Noori[1], Saeid Reza Ameli[2], & Hassan Hosseini[3]

[1]Corresponding author, Department of North American Studies, Faculty of World Studies, University of Tehran, Tehran, Iran; *farnaznoori@ut.ac.ir*

[2]Department of North American Studies, Faculty of World Studies, University of Tehran, Tehran, Iran; *ssameli@ut.ac.ir*

[3]Department of North American Studies, Faculty of World Studies, University of Tehran, Tehran, Iran; *hahosseini@ut.ac.ir*

Received: 17/12/2021 Accepted: 24/10/2022

Abstract

This article focuses on the discursive features of the US securitization of cyberspace in Obama administration. Relying on the Copenhagen school's definition of securitization and using Fairclough's dialectical relational approach to critical discourse analysis, this study is an attempt to see how discourse making was done as part of a securitization process whereby cyber threats were moved to national security arena and led to discoursal militarization of cyberspace. Assuming that discourse making prepares a ground for elite influence, the current study looks into how the US political leaders contributed to militarization of cyberspace between 2009 and 2017 through discourse making which, in turn, paved the way for actual policy initiatives to militarize cyberspace.

Keywords: Critical Discourse Analysis; Militarization; the US; Cyberspace; Securitization.

1. Introduction

Though not explicitly expressed or noticed by common observers, the cyber domain has been pertinent to international relations and military thinking since its early years of existence. As early as 1962, the RAND Corporation began research on "distributed communication networks for military command and control" (Cavelty, 2007, p. 44), and the Advanced Research Projects Agency Network (ARPANET), the precursor of the Internet, was formed in 1960s as "a US Department of Defense project to create a nationwide computer network that would continue to function even if a large portion of it were destroyed in a nuclear war or natural disaster" (Dunn, 2005, p. 6). Cyberspace has always had a military dimension embodied in technological warfare achievements of the Cold War and aftermath. In fact, "the link between *information technology* and *national security* was formed along with and as part of technological achievements in the military domain more than half century ago, when information infrastructures were regarded as military technological advancements" (Ameli et al., 2019, p. 109). Ever since, the issue of information threats to national security has appeared in the US officials' national security discourse, including that of Barack Obama's administration.

Barack Obama was the second US president who took office in the 21st century. After the void the US foreign policy was left with, following the collapse of the Soviet Union, and the security challenges the country was assumed to face in the post 9/11 years, his presidency marks the beginning of an era of building stability and strength over the underpinnings of the security structure shaped throughout twenty years of dealing with a diversity of challenges in lieu of a single adversary and its nuclear weapons. Promising 'change', as his campaign slogan, Obama came to the White House to control the costs US hegemony had incurred by launching two wars in the Middle East, revive the US economy, continue to fight terrorism, restore the international reputation of the United States after it had been injured under Bush and rebuild ties with the East (Canrong, 2016). Added to the challenges of his term was that the US national security apparatus was to include cyber in all areas, from military to economy, and for long-run objectives, to enhance national power and minimize threats. Though not the first US president facing security challenges of the Information Age, the

Obama presidency exemplifies how after a decade of combating new threats, a cyber-inclusive perception of national security priorities translated into actual policy initiatives.

The current article seeks to explore the way the linkage between cybersecurity and national security was reflected in the US officials' discourse in the Obama administration. Given that the inclusion of cybersecurity into national security discussions has been formed and transformed as a longitudinal political process and is one which moves cyber threats to the political sphere and leads to policy decisions at high level politics, this research tries to trace the discursive features of the process under Obama. The author basically argues that the process involved a securitizing discourse in the form of militarization of cyberspace which paved the way for actual policy initiatives to militarize cyberspace.

1.1. Literature Review

Securitization of cyberspace has been studied by scholars either as part of the US cyber strategy or in abstract. Lene Hansen and Helen Nissenbaum's "*Digital Disaster, Cyber Security, and the Copenhagen School*," published in 2009 by International Studies Quarterly has been an influential work for its innovation in drawing a framework for cybersecurity analysis based on the Copenhagen school. Authors explain that the Copenhagen school has three main theoretical roots, "one in debates in Security Studies over whether to widen the concept beyond its traditional state-centric, military focus, one in speech act theory, and one in a classical, Schmittian understanding of the state and security politics" (Hansen & Nissenbaum, 2009, p. 1158). Authors adopt the framework of securitization theory, recon cyber security as a distinct sector with a particular constellation of threats and referent objects. Another argument by the Copenhagen school is that security discourse may constitute other referent objects than the state/nation as threatened and bring in other sectors than the military. Hansen and Nissenbaum (2009) hold that "network security" and "individual security'' are significant referent objects, but their political importance arises from connections to the referent objects of "the state," "society," "the nation," and "the economy." They use the case of Estonia cyber-attacks of 2007 to show that these two referent objects are articulated as threatened through three distinct forms of securitizations: hypersecuritization, everyday security practices, and technifications.

Hansen and Nissenbaum's model has been popular among researchers who would like to study securitization of cyberspace. "*Discourses of cyberspace securitization in Brazil and in the United States"* is the title of an article by Lobato and Kenkel published in 2015. They use the Copenhagen school's theory of securitization and the framework provided by Hansen and Nissenbaum (2009) and suggest the development of a specific analytical security "sector" for cyberspace. Using the US and Brazil as examples, they seek to understand the manner by which discourses of cyber securitization are constructed. They maintain that "governments whose infrastructure and daily lives are highly dependent upon digital networks, as well as think tanks, tend to figure as securitizing actors, for they perceive the destabilization of the networks in which their operations strongly confide as threats" (Lobato & Kenkel, 2015, p. 29). Their primary concern is to discover how some states, acting as securitizing actors before domestic and international audiences, warn about the risks of cyber-attacks and try to bring issues to the security agenda while other states' bureaucracies participate in the construction of the threat. Lobato & Kenkel (2015) compare the securitizing discourse in Brazil and the US, but do not mention any specific research method for their analysis. Table 1 summarizes their data collection sources to compare the securitizing discourse in Brazil and the US.

Table 1. *Data Collection and Sources Used by Lobato & Kenkel (2015, p. 36)*

	Documents	Agencies
USA	1999: A National Security Strategy for a New Century. 2003: The National Strategy to Secure Cyberspace. 2009: Remarks by the President on Securing our Nation's Cyber Infrastructure. 2011: International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World.	Department of Homeland Security • Office of Cybersecurity & Communications • National Cybersecurity Division • Department of Defense • U.S. Cyber Command (USCyberComm) • National Security Agency (NSA)

BRAZIL	2008: National Defense Strategy (Law n° 6.703, 12/18/2008) 2012: Cyber Defense Policy (ordinance n° 3.389/MD, 12/21/2012)	ABIN - Brazilian Agency for Intelligence MD - Ministry of Defense • EB - Brazilian Army • CD Ciber (Center of the Army for Cyber defense) • Presidency of the Republic • Chamber of External Relations and National Defense (CREDEN) • Council for National Defense (CDN) • Department of Informational and Communication Security (DSIC) • The Presidency's Cabinet for Institutional Security (GSI-PR)

Their conclusion presents differences and similarities between the US and the Brazilian securitization discourses. In Brazil, securitization is practiced institutionally under the purview of the president. In the US, the securitization process is consolidated and "permeates governmental practices, serving as a justification for the enhancement of vigilance mechanisms, as well as of state control" (Lobato & Kenkel, 2015, p. 36). Lobato and Kenkel (2015, p. 38) refer to the fact that securitization will be shifted to militarization and since the US is a global power, the discourse which originates there, will shape perceptions of threat in other countries.

The same framework is used by Hjalmarsson (2013) who explores the way the American Government understands and characterizes cyberspace and its relation to security. Relying on the Copenhagen school's definition of securitization and Hansen and Nissenbaum's (2009) framework, Hjalmarsson (2013) takes both a qualitative-intensive method and proposes a quantitative-extensive method to analyze the prevalence of securitizing speech acts in a text corpus. The qualitative investigation demonstrates how securitizing actors in the US government engage in 'hypersecuritization' "by constructing an image of a threat capable of utilizing the networked nature of cyberspace to create destruction on a level that is comparable to previous disasters such as 'Pearl Harbour' and '9/11'" (Hjalmarsson, 2013). Paalman (2013) extends application of the theory by studying effectiveness of discourse making in convincing the audience of the existential threat that cyberspace allegedly poses to the US. He uses discourse analysis to study the speech act of the Office of the President to determine that cyber-securitization has taken place in the period 1998-2012 and measures audience conviction in the securitization framework. His findings indicate that although the share of threat-perception keywords steadily increased over time, with 800% in 2012 compared to 1998, and there was a significant spike from 2009 to 2012, the media is only partly securitized.

Cavelty (2007), too, extends the theory of securitization using framing theory and agenda setting theory and elaborates on the securitization process as a discourse making process which evolved in the US as a result of political procedures. Her book, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age,* is an exploration of "a fairly 'new' security issue in terms of the threat perceptions of key actors and the dynamic interaction between actor constellations, systemic conditions, and institutional settings" (Cavelty, 2007, p. 138). Cavelty (2007) first reviews how cyberspace and national security have been linked together in the United States since Cold War years, and then explains how the first cyber-attacks and crimes strengthened the linkage by shaping threat frames in which IT was regarded as part of national security debates.

Literature produced by other researchers on securitization of cyberspace mostly focuses on the issue as a discursive practice. Theoretically, almost all of them have relied on the Copenhagen school's definition of securitization, but in few researches, 'securitization' is used to refer to practical policy outcomes of discursive securitization. What seems to be missing in literature is a wholescale approach in which securitization is framed as part of national security strategy to see how it contributes to actual policies practiced beyond discourse making. The contribution of this article to the related literature is to regard 'securitization' as a long-term process in which national security objectives are reflected in discourse and are followed by non-discursive consequences.

2. Theoretical Framework

Theoretically, the Copenhagen school and its theory of securitization are used in this work to study the discursive features of the securitization move. For the Copenhagen school, security is created by language and by defining something as a threat to it. Securitization of issues takes place by political leaders in discourse. As Buzan and Hansen (2009, p. 213)

put it, "the definition of security depends on its successful construction in discourse". According to the theory of securitization, securitizing actors, mainly political leaders, "securitize issues by declaring something—a referent object—existentially threatened" (Buzan et al., 1998, p. 36). By defining an existential threat, the securitizing actor legitimizes actions beyond normal political procedures or as Buzan et al. (1998, p. 21) call it "the use of extraordinary measures" to combat the threat. The discursive power of securitization works when actors are in a position "to 'define' security and shape responses to envisaged threats" (Cavelty, 2007, p. 25). The 'facilitating conditions' of securitization, are that: first, the speech act "follows the grammar of security, meaning that it constructs a plot containing an existential threat and a point of no return and offers a 'securitized' way out" (Buzan et al., 1998, pp. 31-33; in Cavelty, 2007, p. 28); second, the securitizing actor should hold "a position from which an authoritative claim about security can be made" (Buzan et al., 1998, pp. 31-33; in Cavelty, 2007, p. 28). So, Securitization is an "essentially inter-subjective process" (Buzan et al., 1998, p. 30) and "ultimately rests neither with objects nor with subjects but among the subjects" (Buzan et al., 1998, p. 31). Any act of securitization needs a securitizing actor, a referent object and an audience.

3. Research Method

To study the discursive features of securitization of cyberspace, critical discourse analysis (CDA) is used as the research method. For CDA, "language is an irreducible part of social life, dialectically interconnected with other elements of social life, so that social analysis and research always has to take account of language" (Fairclough, 2003/4, p. 2). According to Pennycook (2004, p. 787; in Roohani & Tanbakooei, 2012, p. 83), approaches to CDA are concerned with understanding "texts and practices of reading and writing in relationship to questions of social change, cultural diversity, economic equity, and political enfranchisement." CDA is merely concerned with the examination of the dominant culture to analyze elements of injustice, inequality, prejudice and discrimination (Chalak & Ghasemi, 2017, p. 60). In this research, Fairclough's dialectical relational approach (2005, pp. 96-102) to CDA is used as the research method to apply the Copenhagen school's conception of securitization when the referent object of security is cyberspace. As Fairclough (1995, p. 98) states, dimensions of discourse analysis involve the study of linguistic features of the text (description), the discourse practice (interpretation), and the sociocultural practice (explanation). In this research, the securitizing discourse for cyberspace consists of relating cyber security to national security, defining existential threats to national security in cyberspace, expression of the need to take action against the threat and justification of countermeasures outside normal political procedures. In the first layer of analysis, the *description* of the texts involves tracing semantic relations in the texts based on the conceptual definition of securitization of cyberspace. The second layer, *interpretation*, involves relating the texts with social events as to the way the relationship of the agent (author) and the audience figures in representations of facts about cybersecurity, actions as to influence the audience through the text, and identification with the cybersecurity issue in authors' own particular way. Finally, the explanation layer involves the study of how the discursive practice can be regarded as part of the process of securitization of cyberspace and how it reflects practical securitization in the real world.

The texts for CDA can be documents, speeches, hearings, interviews, etc. Due to the huge number of texts, in either form, produced about cybersecurity, texts are selected via purposive sampling. In qualitative research, "samples tend to be as "*illustrative*" of broader social and cultural processes, providing structural coherence within the larger context, rather than generally "*representative*" as in quantitative analysis" (Deacon et al., 1999, p. 43; in Egglestone, 2014, p. 42). This research is a case study of the US militarization of cyberspace and no claims can be made on the generalizability of the findings to other countries' cyber strategy. Thus, purposive sampling, as a non-probability sampling technique, is used to select texts. Figure 1 shows different types of purposive sampling and their features:

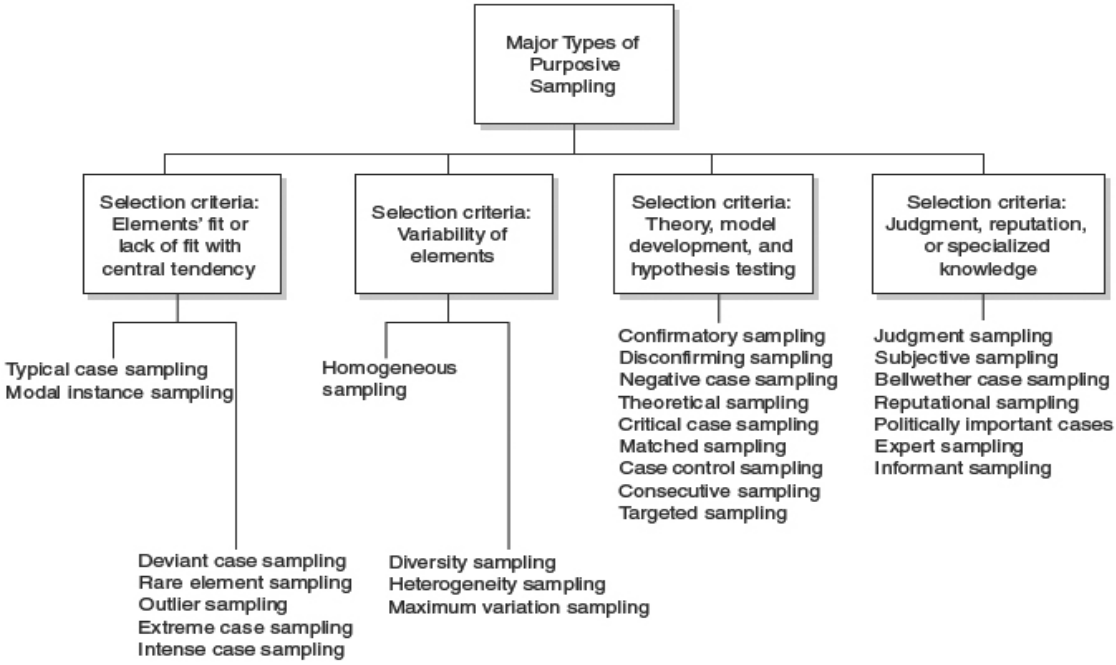

Figure 1. Four Types of Purposive Sampling. Source (Daniel, 2012)

Among the four types of purposive sampling, theory, model development and hypothesis testing, theory is used here for our reliance on the theory of securitization. Indeed, different elements of the theory to explain the securitization process as a speech act are used as below to select texts:

According to Buzan et al. (1998, p. 32), the study of securitization aims to gain an understanding of who (the actor) securitizes which issues (the referent object), for whom or what (the audience), why (the intentions and purposes), with what results (the outcome), and under what conditions (the structure). The main basis for purposive sampling in this research is the theory's application, so sampling is done for texts to be studied to trace discursive features of securitization of cyberspace. Therefore, among the huge population of texts of any type produced in the time period of the research, (2009-2017), purposive sampling was done based on the following criteria:

1. To be reflective of the Copenhagen school's assumptions of the securitization process, selected texts ought to be produced by 'political leaders' to meet the theory's conception of the securitizing actor, (who). Thus, the texts selected were produced by people who could be regarded as "political leaders, bureaucracies, governments, lobbyists, and pressure groups" (Buzan et al., 1998, pp. 40-41). This includes people who were responsible or in charge of official posts or political elite in areas related to national or cybersecurity in the US between 2009 and 2017. The selected texts were produced by Barack Obama (the President), Olympia Snowe (Senator), William Lynn III (Deputy Secretary of Defense), Leon Panetta (Secretary of Defense), Robert Mueller (FBI director) and Mike McConnell (Retired navy admiral). Table 2 lists the selected texts and their authors.

Table 2. *List of Selected Texts*

Text No.	Author	Position	Date Produced
1	Barack Obama	President	May 29, 2009
2	Olympia Snowe	Senator from Maine	Feb. 23, 2010
3	Mike McConnell	Retired navy admiral	Feb. 28, 2010
4	William Lynn III	Deputy Secretary of Defense	Sep. Oct. 2010
5	Robert Mueller	FBI director	Mar. 1, 2012
6	Barack Obama	President	Jul. 19, 2012
7	Leon Panetta	Secretary of Defense	Oct. 11, 2012
8	Barack Obama	President	Jun. 7, 2013
9	Barack Obama	President	Jan 17, 2014

2. Selected texts ought to meet the Copenhagen school's conception of the referent object of securitization, (what). This narrowed down the population to texts produced about cyberspace and cybersecurity.
3. Each of the selected texts enjoys some significance in terms of the author position or time significance related to the context for their production.
4. Selected texts ought to have had a public audience at the time of production to meet the conceptual framework's conception of the audience as the American public, (whom). To this end, the sample includes texts to which free access has been possible for the American public. Also, all the selected texts received vast media coverage at the time of production. None of the selected texts are produced for a limited audience or in private circles.

Besides the textual and processing analysis of the texts in the description and interpretation of each, the production of all of the selected texts studied in this research has to be analyzed within the broader context of a securitization move in the US cyber strategy (social analysis). Unconfined to discourse making, the securitization move context included a vast spectrum of practical measures ranging from establishment of cyber-military institutions to development of cyber weapons. According to Fairclough (1995), explanation of texts in DRA is about the study of the interrelation of discursive processes and social processes. The explanation of the nine texts in this article includes the study of the features of the securitization move, as the context, in relation with and reflected in text production. Although Barak Obama, as a democrat president, made 'change' a campaign slogan to repair the US image worldwide, in national security sphere, his two presidential terms were part of the US grand strategy in early 21st century. Dramatic 'change,' as change in principles of the approach to cybersecurity issues, only took place in the way policies responded to the national security requirements and priorities. Thus, securitization of cyberspace constitutes a long-term process and a context in which text production about cybersecurity took place. The contextual analysis of the strategy needs to be inclusive to a thematic analysis of how the context was reflected in discourse. Figure 2 indicates how Fiarclough's DRA model is used in this research to analyze discursive features of securitization of cyberspace. In-depth analysis of each text is provided in the coming sections.

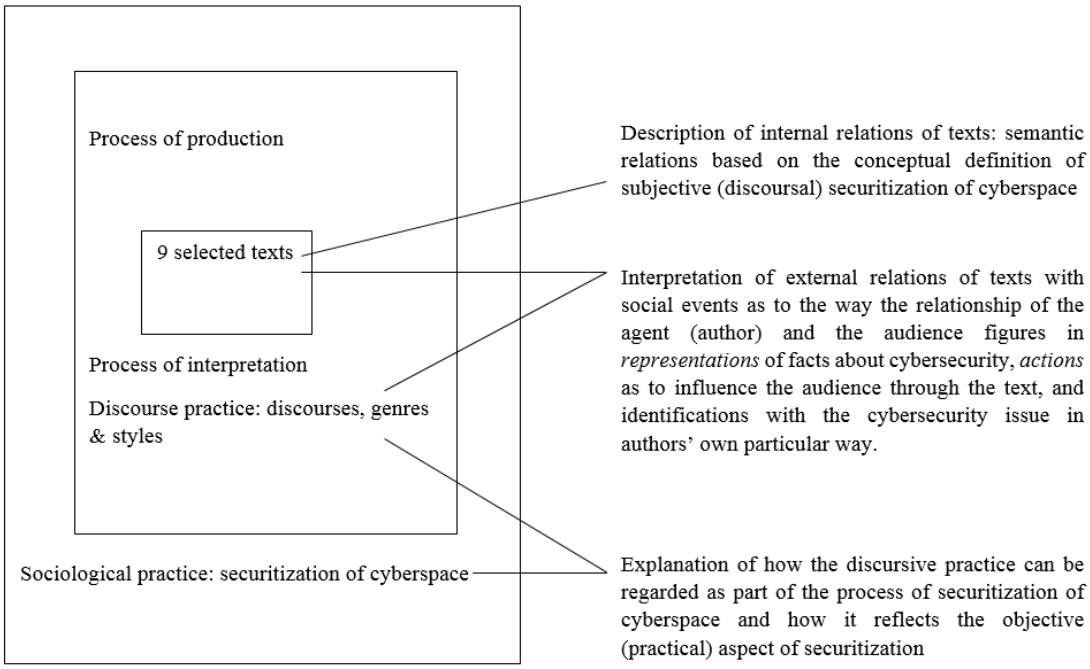

Figure 2. Dimensions of Analysis of the Discursive Features of Securitization of Cyberspace Based on DRA. Source: Authors

4. Findings and Discussion

The following sections summarize findings on the description, interpretation and explanation of the nine selected texts based on the conceptual model presented above.

4.1. Description

The description of texts in this research centers around the study of internal relations of texts, and more specifically, semantic relations. One of the semantic relations traced is problem-solution. It consists of asserting a problem (existential threat to national security in cyberspace) and the solution (countermeasures outside normal political procedures). Embedded in this type of suggesting a problem-solution relation is providing justification for what is not commonly regarded as a normal procedure. The nature of the threat is such that can legitimate the adoption of extraordinary measures. For Berger and Luckmann (1966, in Fairclough, 2003/4, p. 88), "legitimation provides the 'explanations' and justifications of the salient elements of the institutional tradition." The problem-solution relation and the legitimation associated with it are more influential in two ways: first, highlighting the significance of the issue by building other semantic relations such as threat construction about the '*existential'* nature of threat to national security in cyberspace which is built and associated with the use of certain vocabulary building lexical relations or what Fairclough (2003/4, p. 131) calls the use of 'lexical metaphor' or the use of "words which generally represent one part of the world being extended to another"; and second, focusing on what seems to be the only solution to the problem by providing enough justification and reasoning.

In text 1, from the very first sentence, the significance of the Information Age is emphasized describing it as "*a transformational moment.*" Semantic relations are built in different ways about the features of the Information Age and importance of cybersecurity. Obama talks about an "*irony*" and a "*paradox*" of th Information Age:

> *The very technologies that empower us to create and to build also empower those who would disrupt and destroy. And this **paradox** -- seen and unseen -- is something that we experience every day.*
>
> *In this Information Age, one of your greatest **strengths** -- in our case, our ability to communicate to a wide range of supporters through the Internet -- could also be one of your greatest **vulnerabilities**.*

The contrast in meanings of three sets of words, 'create/build' versus 'disrupt/destroy' and 'strengths/vulnerabilities' holds a sense of paradox and implies kind of an irony. Yet, for anyone enjoying some literary and linguistic knowledge, the word irony itself bears a sense of 'uncertainty,' 'nontransparency,' and 'doubt.' It means that two contradictory things are in place and correct at the same time, and it creates a sense of doubt in the audience. The 'irony' needs to be distinguished, discovered and dealt with. The figurative language used helps to intensify the impact of vocabulary:

> *…. our interconnected world presents us, at once, with great promise but also great peril.*

Promise and peril, both start with 'p' and are contrastive in meaning; which sounds like decorating the speech with alliteration and reflecting the 'irony'. Alliteration is also used below to intensify the impact of the promise made by the government to defend the US digital infrastructure:

> *We will **d**eter, prevent, **d**etect, and **d**efend against attacks and recover quickly from any **d**isruptions or **d**amage.*

Obama continues describing different dimensions of the irony. Naming Al-Qaeda a cyber threat, he mentions another instance of this irony:

> *Our technological advantage **is** a key to America's military dominance. **But** our defense and military networks are under constant attack. […]-- attacks that are harder to detect and harder to defend against. Indeed, in today's world, acts of terror could come **not only** from a few extremists in suicide vests **but** from a few key strokes on the computer– a weapon of mass disruption.*

'*But*' creates a contrastive semantic relation: The technological advantage helps the US dominance, *but* there is an obstacle to it. Also, the 'not only … but also' clause creates an additive semantic relation: Terror is possible both through suicide and a computer. The irony is highlighted in both sentences using the two semantic relations to imply that the technology can be a threat. By naming "*a computer*" a "*weapon of mass disruption,*" the irony is solved and brought to the fore: a computer can be a weapon. Reasoning is provided by mentioning the *reality* and *severity* of the threat. If a

computer can be a weapon, it has to be due to its extraordinary capacities. It can cause great damage because nearly everything is dependent upon it.

So cyberspace is real. And so are the risks that come with it.

A semantic relation is made based on the logic of causality: dependence on the Internet and its consequence. The US depends on cyberspace for every vital social, industrial and economic activity and the consequence is that in case of a cyber-attack all those activities and critical infrastructures will be endangered:

*We **rely** on the Internet to pay our **bills**, to **bank**, to **shop**, to **file** our taxes.*

***The small businesswoman** in St. Louis, **the bond trader** in the New York Stock Exchange, **the workers** at a global shipping company in Memphis, **the young entrepreneur** in Silicon Valley -- they all **need** the networks to make the next payroll, the next trade, the next delivery, the next great breakthrough. Ecommerce alone last year accounted for some 132 billion dollars in retail sales.*

*We **count on** computer networks to deliver our oil and gas, our power and our water. We **rely** on them for public transportation and air traffic control.*

Dependence on the Internet for daily social life and critical infrastructures is emphasized by describing the nature of the relation between the US community and the Internet: it is one of **relying**, **needing** and **counting on**. Repetition of the word "*next*" in "*the next payroll, the next trade, the next delivery, the next great breakthrough"* shows how daily life depends on the Internet and at the same time **implies** how basic economic activities of American citizens in different parts of the country, from New York to Memphis to Silicon Valley, will be endangered in case of a cyber incident. The height of the 'dependence' relationship is when national security and economy are involved. A relationship is constructed between cybersecurity and economy and national security:

America's economic prosperity in the 21st century will depend on cybersecurity.

It is noteworthy that the speech was given when America was still suffering from the 2008-9 economic recession and still remembered 9/11 bombings, different interpretations of which had been actively given in 2001 by many political, social and religious institutions (Azimi, 2015). The dependence is also emphasized by certain vocabulary and choice of words. Throughout the speech, Obama uses two phrases to describe the US digital infrastructure:

*a. **the backbone** that underpins a prosperous economy and a strong military and an open and efficient government*

*b. a **strategic national asset***

The depth of dependence of all security and economic challenges on cybersecurity, makes the latter a 'zero-sum' game: either it will be solved or nothing will be solved. Elaboration on the dependence is provided before. Yet, the US president has to deal many security and economic challenges, "*but **none** of this progress would be possible, and **none** of these 21st century challenges can be fully met, without America's digital infrastructure, implying that all of these depend on cybersecurity."* A problem-solution relation exists in the whole text. The first half of the text contains problematization: introducing a problem with all its dimensions and features. Both the irony and the reality-severity relations were part of problematization.

A problem-solution relation lies in text 2, in which author's elaboration on the problem, that is, cyber threats to national security, contains a wide range of dangers as follows:

a. *A burgeoning array of state and non-state adversaries* [who] *are increasingly targeting the Internet, telecommunications networks, and computers*

b. *Malevolent actors* [who] *have actually begun selling counterfeit networking equipment infected with viruses to consumers.*

c. *Breach of electronic records*

d. *Hijacked personal computers, known as "botnets"* [that] *are used to send spam or viruses*

Threat construction is done by elaboration and exemplification about previous cyber-attacks. The author lists a number of recent and familiar cyber incidents in which great damage is brought about either by state actors like China or individuals such as hackers. All the examples are known to the audience and have happened or reported only recently, which helps her push her argument. They include an attack reported in "*an unclassified setting just two weeks ago,*" "*the recent intrusions reported by Google,*" and hackers' gain access to data "*just this week.*" The threat is presented as a very serious one. Language helps the author to emphasize the danger by the use of specific vocabulary. The author uses a lot of adjectives and adverbs to describe the severity of the challenge to national security in cyberspace:

a. *This **exceptional** challenge*
b. *Gravity of these circumstances and the **astonishing** dimensions of this threat*
c. *This **vital** subject*
d. *being assaulted on an **unprecedented** scale*
e. ***Well-resourced** and **persistent** adversaries*
f. ***Extremely** consequential*
g. *A cyber calamity of **epic** proportions, with **devastating** implications*
h. ***Urgent** threat*
i. ***Catastrophic** cyber attack*
j. *This **paramount** issue*

Text 3 produced in the form of an article was published in the Washington Post. The author, Mike McConnell, was the former director of the National Security Agency (NSA) in the Clinton administration and the director of national intelligence during George W. Bush's second term. McConnell moved to the private sector after retirement to work as the executive vice president of Booz Allen Hamilton, one of the biggest companies providing cyber military and intelligence service to the Department of Defense (DoD) and the NSA. He is perhaps one of the people that can be well known as cybersecurity 'experts' in the US machinery of government with a military background. The text starts with threat construction at the very first line:

The United States is fighting a cyber-war today, and we are losing. It's that simple.

The author explains what the features of the cohesive cyber strategy should be. As the solution to the problem, the strategy has to take lessons from the Cold War experience and include *deterrence* and *preemption*: "*Depending on the nature of the threat, we can deploy aspects of either approach to defend America in cyberspace."* For deterrence to work, the US should define clearly its intent and back it up with "*practical policies and international legal agreements to define norms and identify consequences for destructive behavior in cyberspace.*"

Starting with the detailed memory of a cyber-attack on the DoD marks an influential beginning for text 4. The fearful nature of the event is augmented by lexical/semantic relations between rogue, silently, unknown adversary:

*It was a network administrator's worst fear: a **rogue** program operating **silently**, poised to deliver operational plans into the hands of **an unknown adversary**.*

Likewise, problem-solution semantic relation is present throughout the other texts where threat construction is done by mentioning the frequency and probability of threats to the US national security in cyberspace:

Every day, U.S. military and civilian networks are probed thousands of times and scanned millions of times. And the 2008 intrusion that led to Operation Buckshot Yankee was not the only successful penetration. Adversaries have acquired thousands of files from U.S. networks and from the networks of U.S. allies and industry partners, including weapons blueprints, operational plans, and surveillance data (text 4).

Terrorists use the Internet as a recruiting tool, a moneymaker … (text 5)

Terrorists are increasingly cyber savvy (text 5)

Other instances of threat-consequence relation include mentioning different "scenarios' of the most destructive cyber-attacks the US may experience stated in text 7 by Leon Panetta:

> *An aggressor nation or extremist group could use these kinds of cyber tools to **gain control of critical switches**. They could, for example, **derail passenger trains** or even more dangerous, **derail trains loaded with lethal chemicals**.*
>
> *They could **contaminate the water supply** in major cities or **shutdown the power grid** across large parts of the country.*
>
> *The most destructive scenarios involve cyber actors launching several attacks on our critical infrastructure at one time, **in combination with a physical attack on our country**. Attackers could also seek to **disable or degrade critical military systems and communication networks**.*

The solution lies in the US 'new cyber strategy' the headlines of which are elaborated in the second half of the fourth text including the establishment of the Cyber Command and its missions. Supporting the general trends in the new strategy is done by the use of adjectives to describe how the strategy should be:

> *The U.S. government must be modest about its ability to know where and how this threat might mature; **what it needs** is a strategy that provides **operational flexibility** and capabilities that offer **maximum adaptability**.*

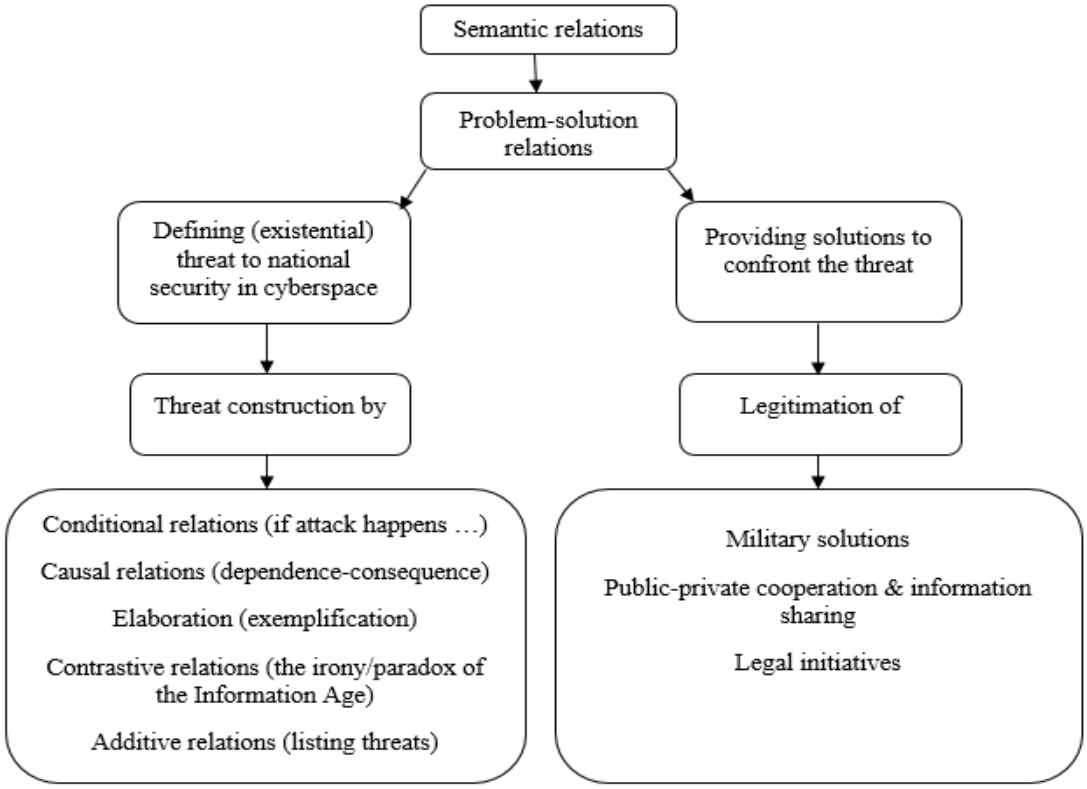

Figure 3. Summary of Findings on Internal Relations of Texts in Description of 9 Texts under Study

The study of the internal relations of the selected texts (description) indicates that semantic relations of different types as pertinent to the conceptual definition of 'securitization of cyberspace in discourse' were present in the texts. Under an umbrella concept of 'problem-solution' relations, the semantic relations existing in the texts consist of relating cybersecurity to national security and economic security and therefore 'threat construction in cyberspace' by creating 1) causal relations (e.g., dependence-consequence relation), i.e. by highlighting the dependence of many critical infrastructures on the Internet and noting the vulnerability of the whole nation and economy to cyber-attacks, 2) conditional relations (e.g., creating disastrous scenarios about what may happen in case of a cyber-attack: 'if attack happens, …' mostly by presenting the threat to national security as 'existential' by the use of lexical metaphors such as warning about a 'cyber Pearl Harbor' and a 'digital 9/11'), 3) elaboration in the form of exemplification about previously

experienced cyber incidents, 4) contrastive relations (e.g., mentioning the irony/paradox of the Information Age as to mark a great technological achievement *but also* threats to nationals security) and 5) additive relations (e.g., listing the different ways in which cyberspace may be a source of threat to national security). In all of these relations, a problem, the cyber threat, was depicted and a solution was provided ranging from legislation to offensive military operation in cyberspace. The solutions provided were justified by 'legitimation' of different types. 'Rationalization', for instance, worked by relying on judgment about the 'severity' of the threats, 'necessity' and 'urgency' of taking actions and 'efficiency' and 'precision' of the solutions provided. Figure 3 summarizes the results of textual analysis of the nine texts in this research.

4.2. Interpretation

Interpretation of texts involves the study of the discursive practice including the analysis of the 'external' relations of texts which is the "analysis of their relations with other elements of social events and, more abstractly, social practices and social structures" (Fairclough, 2003/4) and how these relations figure in Actions, Identifications, and Representations (the relationship of the text to the event, to the wider physical and social world, and to the persons involved in the event: ways of acting (genres), ways of representing (discourses), ways of being (styles)). These three are embodied in the way the relationship of the agent (author) and the audience lets for the text to be interpreted as related to social events at the time of its production and how it aims at:

1. *Representing* the reality/severity/consequence of the threat to national security in cyberspace as related to an event in the real world
2. *Acting* in the form of informing, advising, promising, warning, assuring, persuading, and so on based on the social relationship between the author and the audience
3. *Identifying* with the cybersecurity issue in its own particular way

As for processing analysis of texts discussed in the interpretation of each, this study includes the analysis of the texts as to reveal how the relationship between the author and the audience expressed as '**I, as the … tell you that …**,' was pertinent to the social events in the real world and how the texts contained *representations* of facts in the real world, *actions* as to influence the audience through the text, and *identifications* with the cybersecurity issue in authors' own particular way. Findings indicate that regardless of their positions, the President, Senator, retired navy admiral, Defense Secretary, Deputy Secretary of Defense and FBI director, all authors' representation of the real world phenomenon about cyberspace included **warning** about the threats posed to national security in cyberspace; that is, all the represented facts included some danger to the US national security such as stating that the threat in cyberspace is real and urgent, and that the US is in a cyberwar. This signifies the Copenhagen school's notion of securitization in discourse: presenting a referent object in danger. '*Actions'*, known as what the authors tried to *do* with text differed from case to case, but in sum, all were in line with practical securitization initiatives. Urging for intended legalization and persuading about the military solution are different ways of supporting day-to-day practical securitization measures happening in the real world. Also, author identification with text content and message, defined as creating a commitment based on author sociopolitical position, included giving *assurance* and *promising*, i.e. speaking with certitude, about the practical securitization efforts in the real world. Table 3 summarizes the results of processing analysis for the nine texts covered.

Table 3. *Summary of Findings on External Relations of Texts in Interpretation of 9 Texts Under Study*

Text No.	Position	Representation	Action	Identification
1	President	Cyberspace is real and the threat in it is real too	*Supporting* the content of the 60-day report	Assurance that as the US President he understands the issue and has his own solution to it
2	Senator	The cyber threat is urgent	*Urging* senators to pass the cybersecurity bill	Assurance that as a crossover member of both the Intelligence Committee and the Commerce Committee
3	Retired navy admiral	The US is in a cyberwar	*Advising* government to take urgent & efficient action	Promising that Cold War strategies work to win the cyberwar

4	Deputy Secretary of Defense	Cyberspace is a military domain	*Supporting* the new cyber strategy	Promising that the new cyber strategy helps preserve national security
5	FBI director	Terrorists and criminals are using cyberspace for their purposes	*Convincing* private sector executives for partnership on cybersecurity	Assurance that information sharing with the FBI is to the benefit of the private sector
6	President	Cyber-attacks threaten the US critical infrastructure and economy	*Urging* the Congress to pass the Cybersecurity Act of 2012	Assurance that the solution is in proper legislation
7	Secretary of Defense	Cyberspace is the new frontier	*Urging* the Congress to pass the Cybersecurity Act of 2012	Assertion that the DoD is ready to fight in cyberspace
8	President	There irony about *privacy* and *security* is a fact of modern life	*Justifying* mass surveillance in cyberspace	Assurance that the classified programs are legal and do not threaten US citizens' civil rights
9	President	Cyber intelligence is inevitable	*Convincing* the US community that the government cares for their privacy	Promising change and revision in the programs

4.3. Explanation: Supporting Militarization in Discourse

The third layer of analysis is the study of the sociocultural/sociopolitical practice. It is concerned with the study of how the discursive practice can be regarded as part of the social context in which the text was produced. To do so, a thematic analysis of the texts is done focusing on 'assumptions' in relation with the sociopolitical context in which securitization of cyberspace took place. Assumptions include types of implicitness in a text which connect one text to other texts and to the "world of texts" (Fairclough, 2003/4). According to Fairclough (2003/4), the difference between assumptions and intertextuality is that assumptions "are not generally attributed or attributable to specific texts", they take certain ideas as "common grounds" (Fairclough, 2003/4, p. 41). Fairclough (2003/4, p. 55) distinguishes three types of assumptions:

- **Existential assumptions**: assumptions about what exists
- **Propositional assumptions**: assumptions about what is or can/should/will be the case
- **Value assumptions**: assumptions about what is good or desirable

The Obama administration's discourse on cyberspace and cybersecurity highly supports securitization of cyberspace in the form of militarization. 'Military intentions and aspirations' constitute a basic part of 'existential,' 'propositional,' and 'value' assumptions of all texts under study in this research. The way military intentions were embodied in discourse varied from 'existential' assumptions (presenting cyberspace as a military domain) to 'propositional' assumptions (suggesting military solutions for the threat to national security in cyberspace) and value assumptions (defining an international military role for the US in cyberspace)

4.3.1. Existential Assumptions

Existential assumptions take the military 'nature' of cyberspace for granted. The tendency to support militarization is deeply embedded in the use of military terminology for cyber related issues. Cavelty and Rolofs (in Olszewski, 2016, p. 114) state that the military terminology leads to the conclusion that cyberspace "can and should be recognized as the military-strategic domain [...]. This assumption is problematic and misleading [...] it suggests that countries can establish control over cyber space. It may result in the harmful atmosphere of insecurity and tension at the international level." The nine texts under study contained various instances of the use of military terms to describe 'cyberspace'. An example can be Panetta's phrases to describe cyberspace in text seven as:

a. *the new **frontier***

b. *a new **domain** that we must secure to have peace and prosperity in the world of tomorrow*

c. *a **battlefield** of the future where adversaries can seek to do harm to our country, to our economy, and to our citizens*

d. *a new terrain for **warfare***

The assumption that cyberspace is a military domain is expressed *explicitly*, as in:

*The United States is fighting a **cyber-war** today, and we are losing. It's that simple.* (Text 3)

***As a doctrinal matter**, the Pentagon has formally recognized cyberspace as **a new domain of warfare**.* (Text 4)

and *implicitly*, by comparing military operations in other strategic domains and what needs to be done in cyberspace:

> *We defend. We deter, and if called upon, we take decisive action to protect our citizens. In the past, we have done so thorough operations on **land and at sea, in the skies and in space**. In this century, the United States military must help defend the nation **in cyberspace as well**.* (Text 7)

As other instances, taking cyberspace as "*a **strategic** national asset*" (texts 1, 2, & 4), talking about "***cyber warfare's** threat to the US national security*" (text 4), the possibility of a "*cyber-terrorist attack*" (text 7), and stating that DoD's "*most important investment is in skilled cyber **warriors** needed to conduct operations in cyberspace*" (Text 7) all promote the hype about militarization.

Discourse making by presenting existential assumptions on the military nature of cyberspace is not limited to describing it as a military domain; rather, it moves beyond to make predictions about the future of cyberspace and how it relates to national security signaling warnings about what is to come. 'Cyberwar,' as a military notion, appears in different ways, from talking about the possibility of a new genre of war in future:

> *And last year we had **a glimpse of the future face of war**. As Russian tanks rolled into Georgia, cyber-attacks crippled Georgian government websites. The terrorists that sowed so much death and destruction in Mumbai relied not only on guns and grenades but also on GPS and phones using voice-over-the-Internet.* (Text 1)

(implying that it was Russians and Mumbai terrorists who started the trend and the US is only responding to it), to stating that the cyberwar has already started: "*The United States **is fighting a cyber-war** today, and we are losing. It's that simple"* (Text 3). Asserting that the cyberwar has already started and that the US is falling behind and losing, reminds the Copenhagen school's assumption that "by saying the word, something is done" (Wæver, 1995, p. 55). It automatically results in the conclusion that 'action is needed', erases lines between the military and civilian spheres of cyberspace, moves the whole sphere into a military one and paves the way for announcements such as the establishment of the USCYBERCOM and adoption of offensive military operations in cyberspace. Predictions about the military nature of what is to come in the future in cyberspace is sometimes made by giving references to *enemies* and *terrorists* who are likely to use it as a warfare tool: "*In one hacker recruiting video, a terrorist proclaims that cyber warfare will be **the warfare of the future***" (Text 5).

Cyber terrorism is another notion referred to in the texts as a possible scenario. Panetta mentions that cyberspace may provide grounds for actions of terror to happen: "*Such a destructive **cyber-terrorist** attack could virtually paralyze the nation*" (Text 7). That no such attack has taken place yet, does not impede Mueller from talking about it: "*To date, **terrorists** have not used the Internet to launch a full-scale cyber-attack. But we cannot underestimate their intent*" (Text 5).

Regarding the cyber world as a sphere in which *war* and *terrorism* can be realized, contributes to militarization in discourse in that such existential assumptions implicitly take for granted the war-like situations in cyberspace. While winning in war and combating terror both include active *state* involvement in the form of military presence or policing, predictions about future cyberwar and cyber terrorism legitimize high-level state involvement through arming cyberspace. While many among the public audience may still not have any idea of how a cyberwar or cyber terror look like, the two notions are presented as intrinsic and automatic probabilities embedded in the structure of the Internet: "*The Internet is open. It's highly accessible, as it should be. But that also presents a new terrain for warfare*" (Text 7).

Another existential assumption about the military nature of cyberspace regards cyber as a battlefield in which the US is to face and combat adversaries. The US enemies, from nation-states to individuals to nonstate groups, are given a presence in cyberspace. They are using the Internet and cyber is a front to combat them:

> ***Terrorists*** *use the Internet as a recruiting tool, a moneymaker, a training ground, and a virtual town square, all in one*. (Text 5)
>
> *It is a battlefield of the future where* ***adversaries*** *can seek to do harm to our country, to our economy, and to our citizens.* (Text 7)

According to Buzan et al. (1998, p. 70), the military sector is pervaded by the logic of friend versus foe. The extension of the same mentality into cyberspace by political leaders promotes militarization of the sphere. The idea that 'we are at war in cyberspace' is explicitly mentioned by McConnell as in "*The United States is fighting a cyber-war today …"* (Text 3) and implicitly by Panetta stating that the most important DoD investment is "*in skilled cyber warriors needed to conduct operations in cyberspace*" (Text 7). Given that the digital nature of cyberspace lets for anonymity of users and the fact that following the 9/11 bombings 'terrorism' remained high as the most frightening threat in the American mind, 'being at war with enemies in cyberspace' was easily translated in discourse as *fighting terrorism in cyberspace*. Cyber activities of the terrorist groups with which the US was fighting on the ground were reminded in the texts to support the assumption:

> *Al Qaeda in the Arabian Peninsula has produced a full-color, English-language online magazine.* (Text 5)
>
> *Al Shabaab -- the al Qaeda affiliate in Somalia -- has its own Twitter account".* (Text 5)

Resonating a military tone into speech also took place by depicting cyberspace as a battlefield to which the physical world conflicts are extended:

> *In a future conflict, an adversary unable to match our* ***military supremacy on the battlefield*** *might seek to exploit our computer vulnerabilities here at home.* (Text 6)

Cyberspace is a front in which America has to fight its enemies. The analogy is also present in "*We need to take lessons learned from fighting terrorism and apply them to cyber-crime*" (Text 5), implying that cyberspace has to bear an extension of the physical world counterterrorism operations.

The use of military terminology for cyber related issues was not confined to the use of specific vocabulary, but deeply hidden in the general ideational prompt. A legacy of the Cold War, as a long-term national experience shaping the underpinnings of all US foreign policy in the second half of the 20th century, can be seen in texts in the form of Cold War *terminology* to present existential assumptions on the military nature of cyberspace. McConnell, for example, assumes that the cyber conflicts the US faces and Cold War share a common nature:

> *What is the right strategy for this most modern of wars? Look to history. During the Cold War, when the United States faced an existential threat from the Soviet Union …*

He likens the US strategic environment in cyberspace to the nuclear competition with the USSR and builds an analogy in which enemies pose existential threat to America. The Cold War analogy creates a big opportunity for the use of all kinds of metaphors to talk about cyberspace. The Cold War is associated with the memory of the nuclear threat. A highly military notion, indeed, lags behind the analogy. Brodie (1976, p. 2) calls the invention of atomic bomb "a miracle" and "a revolutionary development which altered the basic character of war itself" due to the destructive power of nuclear weapons. Using the same terminology for cyber-related issues indicates a notorious existential assumption about the military nature of cyberspace. Another example of such analogy is Lynn's way of reminding Albert Einstein's letter to Roosevelt in which he warned about the breakthroughs in nuclear fission as "*aspects of the situation which has arisen seem to call for watchfulness and, if necessary, quick action on the part of the Administration*" and which made Roosevelt prepare the United States for the atomic era. The memory lets for a comparison between the onset of the nuclear age, as the most imperative of the US foreign policy and global dynamics in the 20th century, and the *"the beginning of a new technological age"*, implying that a new war is to come about.

4.3.2. Propositional assumptions

As 'propositional assumptions,' suggesting military solutions for the cyber threat to national security is paramount in the texts and works as another trend for militarization of cyberspace in discourse. Such propositional assumptions are observed as implying that the solution to the problem is a *military* one. It varies from assuming a 'military nature' for the solution to maintaining that there is an inevitable obligation for the military to take part:

> *In an offense-dominant environment, a fortress mentality will not work. The United States cannot retreat behind a Maginot Line of firewalls or it will risk being overrun.* (Text 4)

> *The Department of Defense also has a role. It is a supporting role but it is an essential role. And tonight I want to explain what that means. …. Our mission is to defend the nation. We defend. We deter, and if called upon, we take decisive action to protect our citizens.* (Text 7)

> *Although cyberspace is a man-made domain, it has become just as critical to military operations as land, sea, air, and space. As such,* ***the military must be able to defend and operate within it****.* (Text 4)

A step further is an administrative assumption such as presenting the protection of cyberspace to be the military's *mission*, as text seven in which Panetta's words bear the assumption that cybersecurity is within DoD's jurisdiction as *the* responsible department for cybersecurity:

> *Just as* ***DoD*** *developed the world's finest counterterrorism force over the past decade,* ***we need to build and maintain the finest cyber force and operations.*** *We're recruiting, we're training, we're retaining the best and the brightest in order to stay ahead of other nations.* (Text 7)

Recruitment and training are obviously followed by budgeting and that, per se, institutionalizes the propositional assumption that Pentagon is and should be responsible to protect America's cyberspace. It is Pentagon that makes the cyber strategy and implements it. Moreover, as the Defense Secretary, Panetta appears to talk to and warn the US *cyber* enemies about the consequences of their attack on the US networks:

> ***Potential aggressors should be aware*** *that the United States has the capacity to locate them and to hold them accountable for their actions that may try to harm America.* (Text 7)

The assumption is also taken for granted in Lynn's article about the new cyber strategy: as the threats increase, the Pentagon has started to take action, implying that it was in DoD's jurisdiction to get involved:

> *As the scale of cyberwarfare's threat to U.S. national security and the U.S. economy has come into view,* ***the Pentagon*** *has built layered and robust defenses around military networks and …* (Text 4)

As practical initiatives to militarize cyberspace, decisions like the establishment of the Cyber Command were supported in discourse through emphasis on the necessity of their establishment: "*To facilitate operations in cyberspace, the Defense Department needs* ***an appropriate organizational structure****"* (Text 4). Harmonizing and integration of all military operations in cyberspace was among the objectives of the establishment of the Cyber Command. While the establishment was highly controversial in media at the time the decision was made, it was supported in elite discourse both at the time and in the following years. The arguments about the Command rose in 2009 when Lt. Gen. Keith Alexander, then director of the National Security Agency, was nominated for a fourth star and to take on the top job at the CYBERCOM; a decision which raised concerns among the Senate members about whether the new position could violate laws which prevent the military from operating in domestic issues. Ignoring the concerns, Panetta supports it in his speech:

> *And we're looking at ways to strengthen Cyber Command as well. We must ensure that hit has the resources, that it has the authorities, that it has the capabilities required to perform this growing mission. And it must also be able to react quickly to events unfolding in cyberspace and help fully integrate cyber into all of the department's plans and activities.*

Supporting the establishment of the Cyber Command, as a propositional assumption on the military nature of the solution to the cybersecurity challenge, also took place by trying to imply reasoning on its significance as an element of national pride worldwide: "*Cyber Command has matured into what I believe is a world-class organization*" (Text 7). Lynn describes the situation before the establishment of the Command stating that "*for the past several years, the*

military's cyber defense effort was run by a loose confederation of joint task forces dispersed both geographically and institutionally" (Text 4) and then highlights the Command's significance maintaining that while "*the scale of the effort to protect cyberspace had outgrown the military's existing structures*" the decision was made to integrate cybersecurity operations. Actually the 'new strategy' on which Lynn provides elaboration and support in text 4, is all about the DoD mission in cyberspace including the establishment of the Cyber Command, giving the central role to the Command for cybersecurity.

Another propositional assumption with military implication involves the presence of the Cold War legacy among the suggestions to confront cyber threats. 'Deterrence' and 'preemption', for instance, as two Cold War strategies to combat USSR nuclear threat, are explicitly expressed in McConnell's approach in text three:

> *The **cyber-war** mirrors the **nuclear challenge** in terms of the potential economic and psychological effects. So, should our strategy be **deterrence** or **preemption**? The answer: **both**. Depending on the nature of the threat, we can deploy aspects of either approach to defend America in cyberspace.*

Building alliances worldwide to decrease vulnerabilities and make shared confrontation against the Soviet threat was another Cold War strategy embodied in the creation of North Atlantic Treaty Organization (NATO) as a manifestation of transatlantic alliance against the Communist bloc. The same idea is present in discourse as a suggestion for the US to confront cyber threats:

> *Given the global nature of the Internet, **U.S. allies** also play a critical role in cyber defense. The more signatures of an attack one can see, and the more intrusions one can trace, the better one's defenses will be. In this way, the construct of **shared warning—a core Cold War doctrine— applies to cyberspace**. Just as the United States' air and space defenses are linked with those of allies to provide warning of an attack from the sky, so, too, can the United States and **its allies** cooperatively monitor computer networks for intrusions.* (Text 4)

The tendency of old Cold War strategists to win the discourse and retain their influence over the 'new' domain discussions is a tempting explanation for the analogy. Yet, an initial and more relevant explanation could be that the Cold War legacy, as a long-term victorious competition with another superpower at ideological and military levels, can revive a nostalgic feeling among the American public memory to create, develop and more importantly provoke compromise among the audience that the key solution is in the hands of *generals*. This, can eventually legitimize government policies for cybersecurity. The Cold War mode clearly appears in McConnell's promising tone while trying to assure his audience that relying on that experience will be fruitful and 'working':

> ***We prevailed in the Cold War** through strong leadership, clear policies, solid alliances and close integration of our diplomatic, economic and military efforts. We backed all this up with robust investments -- security never comes cheap. It worked, because we had to make it work. **Let's do the same with cybersecurity**.* (Text 3)

That the end of the Cold War led to the US supremacy as the only world superpower works as an implicit motivation for political leaders to maneuver on its doctrine, tie cybersecurity with militarization in discourse and promise good days provided that the cyber military strategies are implemented. The logic behind it looks as simple as: 'We did it before and we can and will do it again'.

Military thinking about cyberspace is also embedded in the *approach* to deal with cyber threats. Reflecting strategic thought, the idea that 'offense prevails defense' in cyberspace is present in discourse: "*In cyberspace, the offense has the upper hand"* (Text 4). The idea that enjoying destructive offensive capabilities can prevent adversaries from taking action and can work as a good defense, raises from a highly military mentality. Brodie, for instance, as a well-known strategic author of the Cold War years named the atomic bomb "the absolute weapon" (Brodie, 1946, p. 23; in Liff, 2012, p. 414) for there was no defense against it. In 1940s and 1950s America, it was believed that the very existence of nuclear weapons would make deterrence easy due to their destructive power. The same idea appeared in the discourse about cyberspace promoting militarization of the sphere:

> *But we won't succeed in preventing a cyber-attack through improved defenses alone.* (Text 7)

> *Given the dominance of offense in cyberspace, U.S. defenses need to be dynamic.* (Text 4)

Giving priority to offense rather than defense, was implemented in the real world in the form of development of offensive cyber capabilities in order to prevent adversary actions, and was reflected in discourse in the form of support for offensive military operations in cyberspace:

> *In an offense-dominant environment, a fortress mentality will not work. The United States cannot retreat behind a Maginot Line of firewalls or it will risk being overrun. Cyberwarfare is like maneuver warfare, in that speed and agility matter most.* (Text 4)

> *Our cyber adversaries will be far less likely to hit us if they know that we will be able to link to the attack or that their effort will fail against our strong defenses.* (Text 7)

4.3.3. Value Assumptions

'The US should be the dominant military power in cyberspace.' This was a national value voiced as 'assumed' or 'given' in texts. Aspirations for cyber military dominance of the United States is the value assumption contributing to militarization of cyberspace in discourse. The assumption is evidently expressed in the texts as:

> *The United States enjoys unparalleled technological resources, and it can marshal its advantages to create* ***superior military capabilities*** *in cyberspace.* (Text 4)

Regarding cyber as a domain to maintain national power and exert influence worldwide is a common belief among American strategy makers. 'World leadership' is a great motif to regard cyberspace as a domain for power enhancement. There should be no domain left for the only superpower to exert one-way influence. Cyber is a new manmade domain invented as a US technological achievement in the 20th century. The United States should maintain its supremacy in cyberspace and one way to achieve this objective is military superiority in cyber:

> *So a new world awaits -- a world of greater security and greater potential prosperity -- if we reach for it,* ***if we lead****. So long as I'm President of the United States, we will do just that. And the United States --* ***the nation that invented the Internet, that launched an information revolution, that transformed the world -- will do what we did in the 20th century and lead once more in the 21st****.* (Text 1)

The key to achieve military dominance in cyberspace is the US technological asset: "*Our* ***technological advantage*** *is a key to America's* ***military dominance****"* (Text 1). The analogy assumes the US military dominance to be a given value. Just as the technological superiority is absolute, the military dominance should be so:

> *The United States enjoys* ***unparalleled technological resources****, and it can marshal its advantages to create* ***superior military capabilities*** *in cyberspace.* (Text 4)

The superior technology and its contribution to military dominance are also perceived strategically, that is, a value which is translated into a strategy:

> *The U.S. government, therefore, must confront the cyber defense challenge as it confronts other military challenges: with a focus not on numbers but on superior technology and productivity.* (Text 4)

The social analysis of the nine texts under study, presented in a common explanation to all of them, included the study of how the broad sociopolitical practice of securitization of cyberspace was reflected in discourse. Results indicate that 'militarization of cyberspace' was clearly promoted in discourse by political leaders in Obama administration. Categorized under three subsections of existential assumptions, propositional assumptions and value assumptions of the texts, a thematic analysis on the military aspirations in the nine texts indicates the frequency of existential assumptions on the military nature of cyberspace expressed thematically by: 1) suggesting that cyberspace *is* a military domain by using military terminology to describe it such as "a strategic asset" or "a new frontier", 2) predicting events such as a cyberwar or cyber terrorism, as probabilities of a military nature, to happen in the near future, 3) stating that the US is *fighting* enemies in cyberspace which transfers the 'friend and foe' nature of military thought into cyberspace discourse, and 4) presenting cybersecurity issues as a 'Cold War like' challenge using Cold War terminology about cyberspace and making analogies in which the cybersecurity issue is likened to the nuclear challenge. There were also propositional assumptions on the military nature of the solution to the cyber threat to national security. Thematically, they include assumptions in which: 1) Pentagon was represented as *the* responsible Department to deal with the issue implying that the key to the problem was in hands of generals, 2) cyber-military institutions such as USCYBERSOM were supported by elaboration on the necessity of their very existence, 3) Cold War like strategies such as deterrence and preemption

were proposed to combat cyber threats, and 4) offense was presented as having the upper hand over defense in cyber, implying a military thinking about cyberspace. The military value assumption taken for granted was that the US should enjoy being the superior military power in cyberspace. The US 'military dominance' in cyberspace was taken as a given value relying on the country's technological assets. Figure 4 summarizes the thematic headlines of the militarization discourse on cyberspace in the nine texts under study.

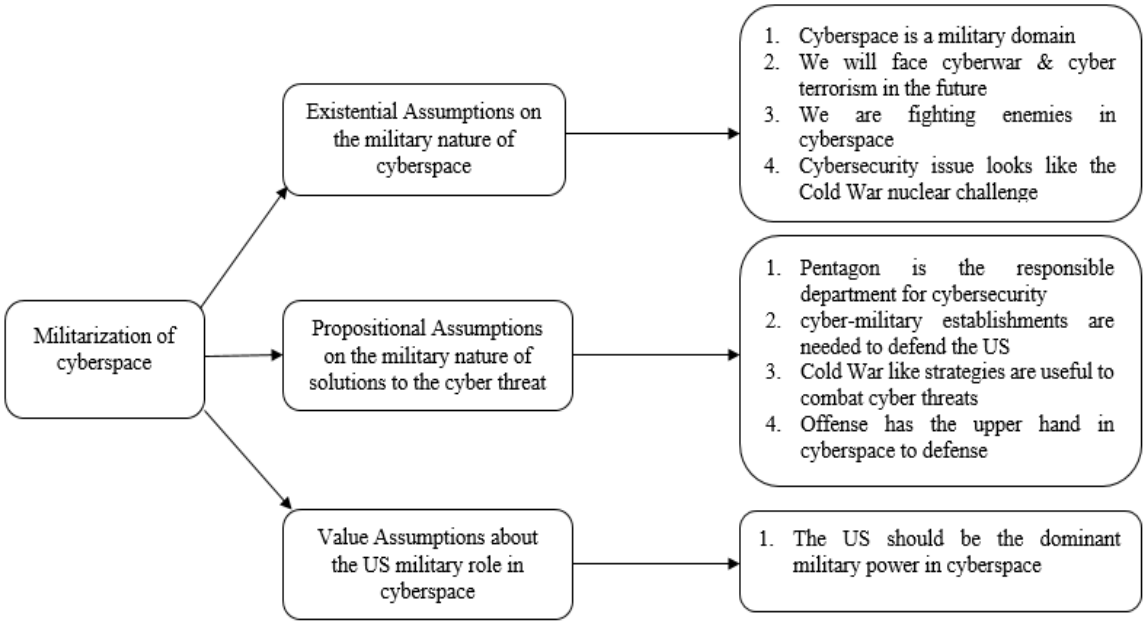

Figure 4. Summary of Findings on External Relations of Texts in Explanation of 9 Texts under Study Regarding Militarization of Cyberspace

5. Conclusion

The previous sections contained a CDA (including text analysis, processing analysis and social analysis) of nine selected texts to trace features of the securitization move in discourse production about cybersecurity in the US in Obama administration. The discussion on how discourse at the three levels contributed to subjective (discoursal) securitization of cyberspace includes a conclusion on the way the interaction of the three layers worked. Figure 5 summarizes the way the three dimensions of discourse contributed to militarization of cyberspace in the US in Obama administration.

A deeper analysis of the political context in which these texts were produced involves an understanding of the way militarization of cyberspace was implemented in practice. As part of the US cyber strategy for the current century, there are strong intents to stabilize the US military dominance in cyberspace for long term national security objectives. Institutionalization of cyber military establishments, vast recruitment and budget allocation indicate '***centralization and hierarchization of US military authority in cyberspace***.' Also proliferation of offensive cyber weapons such as Stuxnet stands for the tendency to pioneer in developing cyber warfare. Given that such establishments: 1. follow long-term objectives, 2. are unlikely to be shut down in succeeding presidential terms and 3. enjoy strong bipartisan support in the Congress, reveal intents for the US military dominance in cyberspace. As the studied texts indicate, the perceived threat in cyberspace was not solely coming from hackers and individuals but also from nation-states, since other nation-states, especially China and Russia, were developing their cyber military capabilities too. The emergence of other state actors with possible military power in cyberspace could threaten the US military superiority in cyberspace. Meanwhile, longitudinal digitalization of basic infrastructures had made the US "a digital nation" (Cyberspace Policy Review, 2009, p. 13) whose critical infrastructure dependence on the cyber made it vulnerable to cyber threats. Moreover, the assumption of the 'leading role for the world' is not void of a cyber variable. Therefore, based on the idea that the US power and influence should dominate in all areas including cyber, the new emerging domain for the exertion of power and influence is regarded to require strong military presence and dominance.

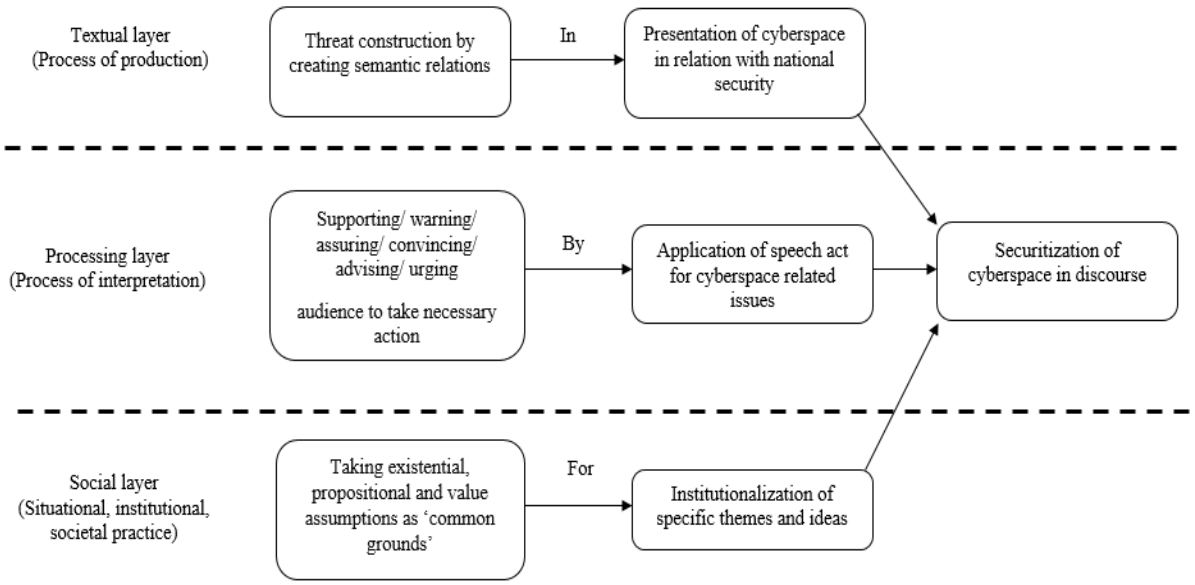

Figure 5. Summary of Findings on the Discursive Features of Securitization

Funding

No funding was received for conducting this study.

Data Availability

The authors confirm that all the data collected or analyzed during this study are included in this published article.

Conflict of Interest

The authors declare that they have no conflict of interest.

References

Ameli, S. R., Hosseini, H., & Noori, F. (2019). Militarization of cyberspace, changing aspects of war in the 21st century: The case of Stuxnet against Iran. *Iranian Review of Foreign Affairs, 10*(1), 99-136.

Brodie, B. (Ed.). (1976). *The absolute weapon: Atomic power and world order*. New York: Harcourt, Brace & Company.

Buzan, B., & Hansen, L. (2009). *The evolution of international security studies*. Cambridge University Press.

Buzan, B., Wæver, O., & de Wilde, J. (1998). *Security: A new framework for analysis*. Boulder: Lynne Rienner.

Canrong, J. (2016). *How America's relationship with China changed under Obama.* Retrieved March 5, 2021 from the World Wide Web: https://www.weforum.org/agenda/2016/12/america-china-relationship/

Cavelty, M. D. (2007). *Cyber-Security and threat politics: US efforts to secure the information age*. Taylor & Francis e-Library.

Chalak, A., & Ghasemi, B. (2017). A critical discourse analysis of four advanced ELT textbooks based on Fairclough's framework. *Journal of Research in Applied Linguistics, 8*, 60-66. https://doi.org/ 10.22055/rals.2017.12869

Cyberspace policy review. (2009). Retrieved March 5, 2021 from the World Wide Web: https://assets.documentcloud.org/documents/2700108/Document-28.pdf

Daniel, J. (2012). Choosing the type of non-probability sampling. In J. Daniel (Ed.), *Sampling essentials: Practical guidelines for making sampling choices* (pp. 81-124). UK: SAGE.

Dunn, M. (2005). *A comparative analysis of cybersecurity initiatives worldwide*. Paper prepared by Center for Security Studies, Swiss Federal Institute of Technology (ETH Zurich) for the WSIS Thematic Meeting on Cybersecurity Geneva (28 June-1 July 2005). Document: CYB/05. International Telecommunications Union.

Egglestone, T. A. (2014). *A critical discourse analysis (CDA) of the contesting discourses articulated by the ANC and the news media in the city press coverage of the spear* [Unpublished master's thesis]. Rhodes University.

Fairclough, N. (1995). *Critical discourse analysis: The critical study of language.* London: Longman.

Fairclough, N. (2003/4). *Analyzing discourse: Textual analysis for social research*. Retrieved 22 April, 2019 from the World Wide Web: http://pirp.harvard.edu/pubs_pdf/ganley/ganley-i93-2.pdf

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

Hjalmarsson, O. (2013). *The securitization of cyberspace; How the Web was won.* Retrieved 22 April, 2019 from the World Wide Web: http://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=3357990 &fileOId=3357996

Lobato, L. C., & Kenkel, K. M. (2015). Discourses of cyberspace securitization in Brazil and in the United States. *Polít. Int, 58*(2), 23-43.

Lynn III, W. F. (2010). Defending a new domain: The Pentagon's cyberstrategy. *Foreign Affairs, 89*(5), pp. 79-108.

McConnell, M. (2010, Feb. 28). *Mike McConnell on how to win the cyber-war we're losing. The Washington Post*. Retrieved 22 April, 2019 from the World Wide Web: http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html

Mueller, R. (2012). *RSA cyber security conference address.* Retrieved 25 April 2019 from the World Wide Web: https://www.americanrhetoric.com/speeches/robertmuellerrsacyberconference2012.htm

Obama, B. (2009). *Remarks by the president on securing our nation's cyber infrastructure. The White House.* Retrieved 22 April, 2019 from the World Wide Web: https://obamawhitehouse.archives.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure

Obama, B. (2013). *Statement by the president.* Retrieved 28 April 2020 from the World Wide Web: https://obamawhitehouse.archives.gov/the-press-office/2013/06/07/statement-president

Obama, B. (2014). *Remarks by the president on review of signals intelligence.* Retrieved 28 April 2020 from the World Wide Web: https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence

Obama. B. (2012). Taking the cyberattack threat seriously. *The Wall Street Journal*. Retrieved 28 April 2020 from the World Wide Web: https://www.wsj.com/articles/SB10000872396390444330904577 535492693044650

Olszewski, B. (2016). Militarization of cyber space and multidimensionality of security. *Journal of Science of the Military Academy of Land Forces, 48*(2), 105-120. https://doi.org/10.5604/17318157.1216083

Paalman, M. (2013). *The Copenhagen school in the fifth domain: Successfully securitizing cyberspace?* Unpublished master's thesis, Uppsala University.

Panetta, L. (2012, Oct. 11). *Remarks by secretary Panetta on cybersecurity to the business executives for national security, New York City.* Retrieved 28 April 2020 from the World Wide Web: https://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136

Rog, J. (2018). *Updating securitization to the age of information: Revisiting Security Sectors by Examining PRISM.* Retrieved 20 April 2020 from the World Wide Web: https://studenttheses.uu.nl/handle/20.500.12932/31079

Roohani, A., & Tanbakooei, N. (2012). Evaluating passages 1 and first certificate textbooks: A discourse perspective. *Journal of Research in Applied Linguistics, 3*(2), 82-106.

Schwarz, K. J. (2016). *The securitization of cyberspace through technification.* Unpublished master's thesis, Virginia Polytechnic Institute and State University. Blacksburg.

Snowe, O. (2010, Feb. 23). *Hearing before the committee on commerce, science, and transportation United States Senate.* Retrieved 28 April 2020 from the World Wide Web: https://www.govinfo.gov/content/pkg/CHRG-111shrg57888/html/CHRG-111shrg57888.htm

van Dijk, T. A. (1993). *Elite discourse and racism.* UK: SAGE.

Wæver, O. (1995). Securitization and desecuritization. In R. Lipschutz (Ed.), *On security* (pp. 46-86). Columbia University Press.