CHARLES UNIVERSITY

FACULTY OF SOCIAL SCIENCES

Institute of Political Studies

Department of International Relations

Cyber Security in the United States of America: Assessing the Role of the Department of Homeland Security

Master's Thesis

Author: Lucie Hofmanová

Study programme: International Relations

Supervisor: Raluca Csernatoni, Ph.D.

Year of defence: 2019

Declaration

1. I hereby declare that I have compiled this thesis using the listed literature and resources only.
2. I hereby declare that my thesis has not been used to gain any other academic title.
3. I fully agree to my work being used for study and scientific purposes.

In Prague on 25.4.2019 Lucie Hofmanová

References

Hofmanová, Lucie. *Cyber Security in the United States of America: Assessing the Role of the Department of Homeland Security.* Praha, 2019. 108 p. Master's thesis (Mgr.). Charles University, Faculty of Social Sciences, Institute of Political Studies. Department of International Relations. Supervisor Raluca Csernatoni, Ph.D.

Length of the thesis: 220 195

Abstract

As one of the major players in cyber security, the United States (U.S.) holds a specific, national security-focused approach towards this field. The most prominent actor in the U.S. within this discipline is the Department of Homeland Security (DHS), which has released its own cyber security strategy four months prior to the overall national strategy. Based on its position in this domain and the specific relationship with the president of the U.S., the thesis aims to explore the DHS and its agenda-setting powers that were used to push its discourse onto the national level. This thesis examines the cyber security strategy of the U.S., specifically the position of the DHS in cyber security, and attempts to determine if this federal department used its influence to mainstream its discourse in the national cyber security strategy. The thesis further analyzes what is the cyber security strategy of the U.S., and if there has been a securitization of this field after 9/11. It draws on a variety of theories and analytical tools, including Hansen and Nissenbaum's securitization theory and agenda setting theory, as well as various methods of political discourse analysis, Fairclough's critical discourse analysis, historical analysis, and process tracing. Ultimately, the thesis reveals the securitizing discourse in DHS documents and demonstrates how it used its agenda-setting power to push its rhetoric into the national cyber security strategy. The thesis also fills the gap in the literature about the position of federal departments and agencies in the U.S. cyber security area. Furthermore, it finds that the national cyber security strategy of the U.S. holds a securitizing discourse which is comparable to the one of the DHS. Finally, the thesis uncovers that the strategy lacks details about the actors who would take charge and execute it. However, it still progresses further than its predecessors, and ultimately recognizes the need for a comprehensive strategy. Additionally, the thesis also concludes that the events of 9/11 served as a strong catalyst to legitimize the securitization of this discipline.

Abstrakt

Jako jeden z hlavních aktérů v oblasti kybernetické bezpečnosti, drží Spojené Státy Americké (USA) specifický přístup zaměřený na národní bezpečnost vůči tomutu odvětví. V rámci USA je jedním z předních aktérů v tomto oboru Ministerstvo pro vnitřní bezpečnost (DHS), které vydalo svoji vlastní kyberbezpečnostní strategii o čtyři měsíce dříve než byla

vydána národní kyberbezpečnostní strategie. Na základě pozice tohoto ministerstva v dané oblasti a jeho specifického vztahu s prezidentem USA, se tato práce zabývá DHS a jeho 'agenda-setting power', kterou využilo k přenesemí své rétoriky na národní úroveň. Dále se zaměřuje na analýzu kyberbezpečnostní strategie USA, specificky na postavení DHS v rámci tohoto odvětví, a snaží se stanovit, zda tento aktér ovlivnil diskurz národní kyberbezpečnostní strategie. Jedna z hlavních otázek je také, jestli došlo k sekuritizaci kyberprostoru v USA po útocích 9/11. Práce využívá řadu teorií a metod, mezi které patří modifikovaná teorie sekuritizace od Hansen a Nissenbaum, 'agenda-setting theory', politická diskurzivní analýza a Faircloughova kritická diskurzivní analýza, historicka analýza, a 'process tracing'. Díky tomu přichází se zjištěním, že se v dokumentech DHS nachází sekuritizující diskurz, který poukazuje na to, jak tento aktér využil svoji 'agenda-setting power' k prosazení vlastní rétoriky v rámci národní kyberbezpečnostní strategie. Tímto také dochází k vyplnění mezery v existující literatuře týkající se pozice ministerstev a federálních agentur v oblasti kyberbezpečnosti USA. Mimo jiné práce dále konstatuje, že i národní kyberbezpečnostní strategie USA obsahuje sekuritizující diskurz, který odpovídá diskurzu DHS v příslušné oblasti. Na druhou stranu, však národní strategie postrádá zásadní detaily, především o aktérech, kteří by měli převzít iniciativu v daném odvětví, nebo jak má dojít k jejímu plnění. I přesto je však krokem kupředu oproti svým předchůdcům, a celkově uznává potřebu po komplexní strategii. V neposlední řadě, práce dochází k závěru, že události 9/11 posloužily jako intezivní katalyzátor, který legitimizoval sekuritizaci kyberbezpečnostního odvětví.

Keywords

Cyber security, the Department of Homeland Security (DHS), USA, Securitization theory, Discourse analysis, National Cybersecurity Strategy, 9/11

Klíčová slova

Kyberbezpečnost, Ministerstvo pro vnitřní bezpečnost, USA, Teorie sekuritizace, Diskurzivní analýza, Národní kyberbezpečnostní strategie, 9/11

Title

Cyber Security in the United States of America: Assessing the Role of the Department of Homeland Security

Název práce

Kybernetická bezpečnost v USA: Posouzení úlohy ministerstva pro vnitřní bezpečnost

Acknowledgement

I would like to express my gratitude to Raluca Csernatoni, Ph.D. for her supervision, guidance, valuable recommendations, and numerous discussions that helped form this thesis. Furthermore, I would like to thank my family for their support during the writing process of the thesis.

Table of Contents

Introduction

Cyber security has become one of the most prominent academic, political, security research and policy areas, which utilizes various concepts, policies, practices, and tools serving the need to protect the cyber environment and its users from distinct cyber risks and threats (ITU, n.d.). The importance of cyber security has grown exponentially since the establishment of cyberspace. Cyberspace could be considered as a new global domain in the information technology infrastructure, which uses the electronics and electromagnetic spectrum in order to create, exploit, modify and store information through independent and interconnected information communication technologies (ICTs) (Kuehl, in Kramer, Starr and Wentz, 2009, p. 28). While cyberspace brought new opportunities in terms of information accessibility, creating new jobs, and facilitating data storage, it has also manifested vastly new national security challenges. As incidents of cyber-attacks have grown, national security policies have required more innovative ways to deflect future threats.

The United States (U.S.) has become a pioneer in the area of cyber security and the mitigation of these threats, being one of the first states with a comprehensive cyber security framework. This has given the U.S. a superior position in the field, and has attracted many scholars to study the subject matter (Hansen, Nissenbaum, 2009; Eriksson, 2001; Lewis, 2005; O'Connell, 2012). The scholarly topics involving cyber security range from catastrophic scenarios of cyberterrorism to the application of securitization theory and discourse analysis to cyberspace. The approach of the U.S. towards cyber security has slightly changed with each executive administration, and with major events in the country. In this regard, the 9/11 events played a key role in changing the attitude towards many areas involving cyber, triggering their securitization. This begs the question if the U.S. cyber security has undergone securitization as well. Additionally, the U.S. released its first national cyber security strategy in 2018, for the first time since 2011. The specific approach of the country towards this field makes this document important, but it also raises the issue of what it entails, whether there is a securitizing discourse within it, and if yes, where could its roots be traced and signified. Moreover, the bigger the field has become, the more actors have been involved in the area. This includes entities such as the military, public, and private sector, international organizations, and non-state actors. Within the context of the U.S., it also includes its federal agencies and departments, which play a crucial role in cyber security. While they are assigned different tasks, including law enforcement, resilience of cyberspace, risk

management, and critical infrastructure protection, together they create a security network for the country.

There are four main federal agencies and departments assigned cyber security tasks – the Federal Bureau of Investigation (FBI), the Department of Defense (DoD), the Department of Homeland Security (DHS), and the National Security Agency (NSA). As cyberspace has evolved, they have gained more power in the respective area of cyber space, and have received more objectives. Specifically, the DHS holds a special position in the field, with its particular responsibilities and focus on developing strategies and providing national security policies in order to protect the U.S. from terrorist threats (The White House, 2001). Additionally, this federal department has always had an exceptional relationship with the president of the U.S., which also reflects a puzzling situation surrounding it. In 2018, there were two major documents addressing cyber security – the cyber security strategy of the DHS, and the national cyber security strategy of the U.S. Taking all factors into account, the question arises whether the DHS had the power to push its own agenda into the national cyber security strategy of the U.S., and therefore, expand its power within the constellation of institutional actors.

This thesis focuses on the analysis of the U.S. cyber security strategy, and mainly on the role of DHS in this field. It also tries to identify the focal points of securitization in this area, specifically following the events of 9/11. As one of the main objectives, it sets out to determine whether this federal agency helps and continues with the securitizing discourse in cyber security, and if it used its powers in this area to push its agenda onto the national cyber security strategy. Thus, there are three main research questions: 1) What is the cyber security strategy of the U.S.? 2) Has there been a securitization of cyber security after 9/11? 3) Is the DHS successfully setting the cyber security agenda on the national level? The DHS was chosen as a case study because it is responsible for a large number of cyber security tasks, it is a leading federal department in this field, and it is assigned to provide national security to the U.S., which gives ita special agenda-setting position in the security area. This could potentially reveal whether there is a securitizing discourse with cyber security in the U.S., and tracing the events that served as focal points of securitization could reveal an explanation of the specific position of this country towards this area. Moreover, it provides a temporal outlook over the evolution of this field in the U.S., as well as the position of the DHS and its internal structure, focusing on cyber security, as well as its agenda-setting power, and its impact on the national cyber security strategy.

This thesis proceeds as following. First, is a literature review, identifying gaps within the existing literature in the related topics, and justifying the significance of the chosen subjects for this thesis. The next chapter is the theoretical approach, explaining securitization theory and its adaptation by Hansen and Nissenbaum; agenda-setting theory, along with the description of the terms cyberspace and cyber security, which are a central part of the topic. The main contribution of the thesis lies in demonstrating the agenda-setting power of the DHS, and the ongoing discourse in the area of cyber security in the U.S. Then, the methodology illustrates analytical approaches applied in the thesis, including political discourse analysis, Fairclough's critical discourse analysis, historical analysis, and process tracing. Operationalization follows these lines, clarifying the focus of the thesis, research questions, and use of literature, as well as the outline of the analysis and how it proceeds. The consequent section consists of several parts.

First, it presents the historical analysis of the establishment of the DHS, the first attempts to regulate cyber security and the effects of the 9/11 on them. Then, it examines cyber security, and DHS after 2001, their evolution within each administration, along with the process tracing of 9/11 and its impact on cyber security. The following chapter demonstrates the position of DHS in the field of cyber security by outlining its cyber related divisions and their internal structure. Together with other federal agencies and departments including the NSA, the FBI, and the DoD, tasked with certain cyber objectives, it will later be used to manifest the specific role of the DHS within this field. Next, the thesis analyzes the presence of securitizing discourse in DHS documents by using political discourse analysis, with the methods of Fairclough's critical discourse analysis. It looks for the elements outlined by Hansen and Nissenbaum in their adaption of securitization theory. After that, it proceeds with the same examination on the National Cybersecurity Strategy of the United States of America which presents the current national approach to cyber security. Then, the thesis compares the rhetoric found in the documents by DHS to the discourse in the national cyber security strategy, which illustrates whether this federal agency possessed enough agenda-setting power to push its ideas onto the national level. Finally, all the findings are summarized, giving conclusions to the set research questions.

The next chapter presents a literature review which maps the existening literature in the area of cyberspace and cyber security in the U.S., and identifies the gaps in this respective field. It further demonstrates the focus, and topics covered by academic scholars, while also providing an explanation for the topics in this thesis.

1. Literature review

Cyber security is a dynamic political and academic field that has been gaining importance since the emergence of cyberspace. While bringing many benefits such as better interconnectedness and being able to access information from anywhere in the world, it has also shown its downsides. Cyber threats have been a potential danger that needs to be tackled. Therefore, nations have started working on their own cyber security policies in order to address and solve such issues. The leading country in cyber security has been the U.S., one of the first countries to put forward a cyber security framework. Because of its interest in the field, it consists of wide range of literature and authors, as well as encompassing a wide scope of information and data. Many other countries are slowly starting to uncover this policy domain, but do not have such a strong starting base as the U.S.

In recent years, cyber security has been a widely studied area due to its increased strategic importance. This has been especially true in the case of the U.S. and the emphasis on the possible threats to its critical infrastructure. Several trends can be identified in the scholarship dedicated to cyber security and the case of the U.S., namely dangers to critical infrastructure, cyberterrorism, cyber Pearl Harbor, securitization of cyberspace, construction of cyber threats, or specific approach of the U.S. to cyberspace. These will be further examined in this section in order to identify possible research avenues. Special attention will be given to securitization of the field, due to the fact that it is employed within the thesis which looks for the securitizing discourse within the documents by the DHS and in the national cyber security strategy, it constitutes a significant part of the literature, and in the case of the U.S. it might be one of the most applicable approaches.

As Kenneth Geers (2009) argues, the possibility of an attack by computer hackers is profound and only a question of time. He presents the critical tools by which the infrastructure could be hit, as well as two empirical cases demonstrating the danger of cyber threats, namely the Israeli cyber-attack from 2000, and the Estonian cyber-attack from 2007. Sean M. Condron (2006) comes to a similar conclusion concerning cyber security. While pointing out the current focus of the United States on civil liberties at the expense of national security, he reveals that by not providing enough protection to the computer systems of the national critical infrastructure, it could lead to possible catastrophic scenarios. Furthermore, he underlines the applicability of the law on cyberspace, while demonstrating the blurred lines between defense and security in cyberspace.

The problems with the distinction lead to a confusion since the words are often used as synonyms, and especially in the executive branch where it can cause issues with internal-external security nexus. Moreover, these terms rely on differentiation based on the geographical borders which are not present in cyberspace (Condron, 2006, p. 408-411). The need for protection of the critical national infrastructure has also been emphasized by several other authors (Cordesman, 2002; Gasper, 2008; Rudner, 2013; Lewis, 2014).

The threats to the U.S. critical national infrastructure are often tied with the perils of cyberterrorism. For instance, Lopamudra Bandyopadhyay (2001) has shown the potential dangers of cyberterrorism, as well as discussing the tools, outcomes, and capabilities required to execute such an attack. It has been further stressed that there are ways to deal with these plausible situations with precaution, by implementing preventive measures such as surveillance, a clear response doctrine, improving tools for cyber warfare, or developing a clear framework. This view is shared by Irving Lachow (2009), who conducts an assessment of definitions of cyberterrorism, as well as a framework concerning this issue, and tries to explain why terrorists would be interested in the use of computer networks. He concludes that terrorists are using these tools in order to damage the interests of the U.S., and therefore, there is an urgency for the formulation of the right strategy to counter these actions. Several other authors agree with this viewpoint (Ways, 2005; Harrop, Matteson, 2013; Sales, 2012).

Yet, most of the authors differ in their opinions concerning the severity and even the feasibility of possible cyberterrorism attacks. Gabriel Weimann (2005) studied the viable risks of a real cyberterrorist attack by reviewing previous works on the same topic, trying to distinguish terrorists from hackers and assessing the definition of the term cyberterrorism. It is argued that future terrorists might turn to the use of cyber tools to inflict damage, however, at the moment, they have not chosen this option. According to the author, the problem should be addressed without inflating its significance. Ayn Embar-Seddon (2002) holds the same stance and argues that the threat is undeniable, but it should not be overemphasized. She analyzes the term cyberterrorism, its capabilities, and the manners in which computer systems can be used. She further concludes that while computer systems are vulnerable and are currently used by terrorists, they might not be used to cause physical damage, but rather to spread influence and gain funding. Other authors establish different theories ranging from opinions that cyberterrorism is not posing a threat; terrorists do not have the technical skills to use the sophisticated techniques to inflict damage; to

the issue of cyberterrorism as overestimated, yet, it ought to be viewed with precaution (Weimann, 2004, b; Furnell, Warren, 1999; Stohl, 2006; Lewis, 2002; Kenney, 2015).

Cyber threats in the U.S. are often perceived as catastrophic scenarios. Terms such as 'electronic Pearl Harbor', 'digital Pearl Harbor', or 'Cyber doomsday' can be found in the literature (Stohl, 2006; Lawson, 2011; Rid, 2012; Lawson, 2013). There are discussions whether or not this scenario could be enacted in reality (Lewis, 2003; Gartzke, 2013). Sean T. Lawson, Sara K. Yeo, and Haoran Yu (2016) investigate 'fear appeals' such as the various cyber doom scenarios, and their effects on the cyber security debate (Lawson et al., 2016, p. 68-70). They analyze the tweets about the fictional docudrama by National Geographic '*American Blackout'* in order to study the reactions of the audience and their perception of cyber related matters after watching the show. They suggest that fear mongering can have counterproductive effects because 'it downplays the importance of the real threat'. It is also argued that these potential threats are not likely to turn into warfare and by themselves might not achieve great gains. As shown by Erik Gartzke (2013), by analyzing warfare in cyberspace and its implications, the scenario of a Cyber Pearl Harbor is difficult to execute without physical damage. According to the author, cyberwar will rather be an adjunct element of traditional warfare. It expands the traditional perspective of warfare, which has traditionally taken place on the battlefield. Cyber war presents a new type of war outside of this traditional area, taking place in the digital domain of cyberspace. This further involves new kinds of capabilities, as well as strategies and means to lead such war. Concerning cyber security, it presents a first line of defense (including prevention, frameworks, strategic planning, etc.) against cyber-attacks, which are inherently part of cyber war.

In the context of the U.S. cyber security policy, there has been a significant amount of literature using the securitization framework to examine whether the cyber security field itself has been securitized, if so why it has occurred, or how the cyber related threats are framed and portrayed (Cavelty, 2007; Nissenbaum, 2005). For instance, Johan Eriksson (2001) applies securitization to cyberspace, and argues that the securitization of the sector has already taken place in the 1990s. He further claims that the dangers of cyberspace have been known since it was created. Based on that, the author further attempts to explain why securitization started much later. He ascribes the cause to several factors starting with the end of the Cold War. Given the specific nature of the securitization theory, some authors adjusted it as regards the nature of cyberspace. Lene Hansen and Helen Nissenbaum (2009) adapted the 'grammar' of securitization to cyber

security by adding three elements: 1) hypersecuritization, the plausibility of a catastrophic scenario is highly securitized, although it has not happened ever before, but the contingency is too high; 2) everyday security practice links the threat to the public to make them feel concerned with their own security so they get mobilized; 3) technification, emphasizing the need of expertise and knowledge, thus giving a privileged role to the experts in the field (Nissenbaum, 2009, p. 1164-1168). By expanding the theory of securitization to cyberspace, this framework allows for a broader application of the theory to areas that were not initially considered significant. Moreover, it is a highly specialized field that requires a modified theory that would better reflect its nature. For these reasons, Nissenbaum's approach (2009) is a noteworthy addition to the theoretical framework of cyberspace.

The same approach was pursued by Ralf Bendrath, Johan Eriksson, and Giampiero Giacomello (2007), who have also extended the securitization theory into 'threat politics'. This concept is widened by three factors: frame characteristics, framing actor(s), and contextual conditions. Threat framing theory allows for different perceptions of security other than 'life-or-death' situation. The same theory can be applied to cyber threats, which are, according to the authors, often framed in alarmist manner. The authors have compared the focus of two U.S. presidential administrations in cyber security – the Clinton administration and the Bush Jr. administration before and after 9/11. The securitization discourse was identified during both administrations, but during the Bush Jr administration, it was put into action and did not stay only at the discussions level. The 9/11 attacks served as a focal point for emphasizing the protection of national security and therefore also securitize cyberspace. Drawing on both approaches, Myriam Dunn Cavelty (2008) has used securitization theory in combination with the threat framing theory in order to explain the conflicting nature between the gradual importance of cyber threats and their missing appearance in reality. She concludes that the cyber threats debate is the case of a failed securitization because there are no exceptional measures (policy, strategy, etc.) concerning cyber threats, trying to resolve the governance of cyberspace.

Securitization draws on discourse analysis, which has been also used to explain the construction of threats in cyber security (Deibert, Rohozinski, 2010; Betz, Stevens, 2013). David Barnard-Wills and Debi Ashenden (2012) made use of the governmentality theory and discourse analysis to clarify how the threats in cyberspace are constructed. The discourse causes the militarization of cyberspace, while by describing it as a national security threat it allows the

application of measures that may be harmful. This also moves it out of the reach of the regular government, towards the 'behind-the-door' type of decision making. Cyberspace can also be affected by various influences, which add to specific perceptions such as ungovernable, unknowable, 'making us vulnerable', threatening, and inhabited by threatening actors (Barnard-Wills, Ashenden, 2012, p. 7-10). As well, Myriam Dunn Cavelty (2013) combines securitization theory and discourse analysis to identify the central threat representations of cyberspace and connects them with specific cyber security policies and practices. As stated by Cavelty, there are three major representations: describing malware in biological terms, the depiction of hackers, and the connection between the vulnerability of complex systems, critical infrastructure and the cyber force (Cavelty, 2013, p. 106-115). Cavelty's research has shown that there are different actors (military, civil defense, business actors, security experts, and other state and non-state actors), which shape these particular representations that are in turn accomplished with specific linguistics means. The portrayal of threats by them differs as well. The stress is put on the linkage to the body of the state, the interconnectedness and the connection with the military language. By linking cyberspace to military imperatives, it may imply that it should be dealt with by military personnel. Furthermore, by solely employing discourse analysis, Sean Lawson (2012) evaluates different discourses within the context of the U.S and in relation to the military domain. The term 'war', and the analogy between cyber conflict and the Cold War are the main tendencies found in the U.S. rhetoric. They result in the diversion from the serious issues and further compromise the acceptance of the required measures. The author argues that these war-related terms need not to be framed in the context of cyberspace, which would ultimately allow for a better policy approach towards cyber security.

Several authors also emphasize the fact that the U.S. holds a specific approach towards cyber security (Lynn, 2010; Gjelten, 2013). For instance, James A. Lewis (2005) identifies the cyber security of the U.S. as an 'anomaly' (Lewis, 2005, p. 1), due to the fact that it was not governed like other security areas of Homeland Security, although there was a fearful rhetoric of a 'digital Pearl Harbor'. He demonstrates that the anticipated vulnerable spheres are not as vulnerable as it is often argued. He outlines five sectors - utilities, public safety, transportation, finance and manufacturing - and shows the preventive measures they have taken in order to protect themselves from possible cyber-attacks. The author suggests that the U.S. government should consider how to delineate security policies, proper legislation and regulations, especially for key

areas. The U.S. also often relies on military capabilities when dealing with threats. This may indicate that cyberspace and its related issues should be tackled by military and military actors only. Furthermore, the actual threats may often be of a different character that does not require military capabilities, and thus, may prevent effective countermeasures to be put into place. In this regard, Mary E. O'Connell (2012) focuses on the growing militarization of cyber security, especially in the case of the U.S., where the Department of Defense (DoD) started becoming one of the key agencies for dealing with this area. She further explores the legal issues surrounding cyber security such as the applicability of the international law. Her research presents different countries and agencies that have militarized cyber security, as well as used practices serving to secure cyberspace without the use of military force. The author further emphasizes the protection of cyberspace and its need to be moved from the military sphere and to be governed through peaceful means.

The literature on cyber security in the U.S. includes different areas and theories. In general, it is mostly concentrated around the military field, national security, the development of the cyber security in the context of the U.S., terrorism, or securitization from the point of national security. Furthermore, there is no consensus in the scholarship dedicated to cyber security and the U.S. Although, there are various topics as illustrated above, there is not a unified view within them, and there can be conflicting. This could be seen in the case of the 'cyber Pearl Harbor' issue, where one group of authors perceives it as a serious threat, while the other recognizes it as an unrealistic and hypothetical scenario. Since the U.S. is the nation with a serious concern about cyber security, leading a way in legislative steps, and institutional responsibilities in the area, it is natural that the highest numbers of contributing authors tackle such issues. Moreover, a specific U.S. approach can be identified, concentrated around certain areas, as compared to for example European Union (EU). In the EU case, the concern is more with the protection of privacy rather than national security (Christou, 2017). For these reasons, the literature review considered only literature focusing on the cyber security in the context of the U.S.

The frequent use of securitization theory among the scholar in the cyber security field can be justified by its specific nature. First of all, it is often explained in military or national security terms. That gives it a predisposition for securitization because it feels like it should be dealt with by officials, military personnel, national security advisors etc. Secondly, it is an area in which there is a need for a certain amount of knowledge, and could be even considered an expert based field

in which people without expertise have almost no say. Lastly, it is highly emphasized as problematic since ordinary citizens are constantly reminded of the dangers it may bring to them in the future. Nations are getting ready for a hypothetical scenario of cyberattacks, which have never happened on such a scale that would bring them down. The fearful rhetoric has spread across the nations and is inherently present in the U.S. discourse on cybersecurity.

A significant amount of cyber security issues is tackled by the federal agencies and departments such as Federal Bureau of Investigation (FBI), the DHS, and National Security Agency (NSA). They are the ones dealing with protection, prevention, and investigation of cyberattacks and cyber security. Literature concerned with this topic is rather limited which opens up a gap that should be filled since these institutions are one of the main actors in the area. This thesis aims at filling this gap by closely examining the position of the DHS in the field of cyber security in the U.S. It is one of the federal departments undertaking various tasks concerning cyberspace. Since securitization has been mostly concentrated around national security, the thesis would also contribute by enhancing the scope of actors, which can securitize certain policies or a specific field, to federal agencies and departments.

2. Theoretical approach

This chapter presents the securitization theory and its modified approach by Lene Hansen and Helen Nissenbaum. Furthermore, it introduces the basic explanation of agenda-setting theories, more specifically policy agenda setting. Both of the theories are then applied to the U.S. government's security strategy, discourses of other officials, and the documents of the DHS related to cyber security and cyberspace after 9/11. This provides the thesis with the theoretical basis that is used in later chapters to analyze and evaluate whether the DHS influences the discourse and policy agenda, as well as how the U.S. cyber security strategy is being framed. Moreover, by showing the agenda-setting powers the DHS gained after its establishment in the cyber security area, it may reveal its privileged position in the U.S. cyber security field. The thesis further examines the structural and contextual conditions, which led to the establishment the DHS after 9/11, and the perception of cyberspace and cyber security as shaped by this important event in the U.S. history. This presents the explanation for possible shifts in the socio-political attitude towards cyber security in the U.S., specifically towards the DHS, and the capacities it holds in the field. Furthermore, the chapter clarifies and discusses the key concepts that are used in the thesis to allow for better understanding of the topic.

2.1. Securitization theory

The end of the Cold War brought about a need for new approaches to security since the new threats started emerging, and classical theories could not fully explain them. New theories such as feminism, postmodernism, or postpositivism brought original perceptions to security studies as well as international relations. Another one of these approaches was created by the Copenhagen School, which introduced the securitization theory. It presents a synthesis of classical political realism in international relations and constructivist approaches. The thesis applies its modified version as proposed by Lene Hansen and Helen Nissenbaum (2009), which will be further developed in the next section of this chapter. It extends the original theory developed in the 1990s by Ole Wæver (Balzaq, Léonard, Ruzicka, 2016, p.518; Buzan, Wæver, Wilde, 1998). The following section discusses the classical theory. According to the theory, public issues can be either non-politicized (outside of state and public discussion), politicized (within the state and public discussion), or securitized, which are characterized as existential threats to the referent object's survival, constructed through the speech act (Buzan et al., 1998, p. 23).

Therefore, securitization is a rhetorical act that allows for the use of extraordinary measures that would not be accepted under regular circumstances (Buzan et al., 1998). In order to securitize an issue, a securitizing actor (possessing the securitizing power such as government officials, public entities, or anyone retaining political power) presents the issue as an existential threat to the referent object (an object which is threatened by the issue), to the audience (its composition depends on circumstances under which the issue is securitized), which needs to accept it as such (Balzaq, Léonard, Ruzicka, 2016, p. 495-496). The referent object can constitute anything from society, infrastructure, to state or state's sovereignty. However, the role of the audience is not really defined in the original theory (Balzaq, Léonard, Ruzicka, 2016; Buzan et al., 1998, p. 26-31), thus, it can be difficult to evaluate the importance of the acceptance by it, as well as its role. Also in the case of securitizing actors, there is not a full agreement who or what can constitute such an entity (McDonald, 2008). If the securitization is unsuccessful, it is then described only as a securitizing move (Buzan et al., 1998, p. 26-31). In addition, some authors further suggest that the context can also play a part in successful securitization (Balzaq, Léonard, Ruzicka, 2016). Just as securitization frames an issue as a threat, desecuritization reverses this process by moving it from 'the threat-defense sequence' into normal public sphere of discussion (Taureck, 2006, p. 3). This process is perceived as a preferred long-range option (Waever, 1995, p. 29; Buzan, Waever & Wilde, 1998, p. 29). On the other hand, the securitization theory was often criticized for several things. Firstly, it was often argued that the term 'security' is defined too strictly or narrowly, focusing only on the act as a description of threats to security (McDonald, 2008, p. 564). The thesis overcomes this obstacle by concentrating on cyber security, and applying Hansen and Nissenbaum's approach, which extends the classical theory to a new area of security. Secondly, the securitizing actors usually constituted of dominant actors such as political leaders (ibid). In this case, the range of these actors is widened by also focusing on institutional actors like federal agencies and department, which were not initially considered to be such entities. Thirdly, the context of the act was delineated too narrowly, and concentrated solely on the securitizing moment (ibid). In order to surmount this critique, the thesis explains the structural and contextual conditions which established the DHS after 9/11, as well as this focal moment in the U.S. history and its implications on the perception of cyber security and cyberspace. Lastly, the audience and its importance are tackled to show their significance in the process of securitization.

Initially, the theory was intended for five sectors: economic, environmental, military, political, and societal (Buzan et. al, 1998, p. 7-8). Yet, as it became a more relevant approach, its elements started appearing in new and unforeseen fields. Cyber security belongs to one of those new areas, however, it is questionable whether it is a separate sector of its own, or whether it could fall under one of the original sectors because their boundaries were not specified. For instance, since cyber security often uses the military terminology, the capacities related to the military, and it is often regulated by this body, some might argue it is part of the military sector. On the other hand, its unique character makes it difficult to include it in the traditional sectors.

2.1.1. Hansen and Nissenbaum's adaptation

Some authors have argued that the specific nature of cyberspace requires an adapted approach that would better capture its intricacies. First, Lene Hansen and Helen Nissenbaum (2009) modify the securitization theory as such by adding three elements. First, hypersecuritization presents the possibility of a catastrophic scenario which is highly securitized, although, this situation has never happened before. The process of securitization usually occurs after the event happened which allows for the legitimization of exceptional measures. In this case, the sheer plausibility is excessively high which constitutes a problematic scheme (Hansen, Nissenbaum, 2009, p. 1163-1165). This leads to a redefinition of several terms. Under normal circumstances, threats and risks become 'dangerous' after they are materialized, and security tries to prevent them from happening. However, in this situation, the security is enhanced, although nothing similar has ever happened before. In a sense, security becomes preventive which raises questions whether anything can become a risk or a threat. It further changes perceptions on security, which is no longer defined only as a national security but it is spread into new areas such security of the individual, human security etc. Moreover, the possibility of a catastrophic damage (although there is not an agreement on this topic) is so emphasized that it may start appearing as life-threatening, irreversible and uncontrollable. Thus, this can lead to the legalization of drastic measures that might prevent the future events. Second, everyday security practice connects the individuals and the threat by making them worry about their security in order to get them involved, mobilized and share the common experiences of threats (ibid, p. 1165-1166). By doing this, it becomes easier to present exceptional measures to the public because they think it is for their protection. The DHS may use this in order to get the support for their perception of cyber space and threats surrounding it. Lastly, technification gives a privileged position and role to experts in the field by stressing the

importance of specified knowledge and expertise. It further grants them the ability to present cyberspace, cyber security, and its related issues to the public and push onto it their own perception. This creates a situation in which the experts can become the securitizing actors, and help convince the audience by securitizing scientific speech about the need for passing extraordinary measures (ibid, p. 1166-1168). It also allows for smaller numbers of people to influence the area, and attempt to comprehend its issues.

Overall, this approach better reflects cyberspace rather than the original securitization theory since it was tailored to suit its complex nature. Moreover, the classical theory does not deal with the securitization of a mere possibility of a catastrophic scenario but only the situation in which it has already happened. As it was discussed, it also redefines security, threats and risks and what can pose them. The DHS may also be altering the definition of these terms by attempting to present its own interpretation of them. Furthermore, it stresses the importance of the expertise of the cyber security field which is a crucial aspect of cyberspace. The same logic might be applied to different cyberspace branches within the DHS, and its internal and external experts who retain such knowledge. It further affects the perception of the field, and allows for a better control over securitization of the cyber security since common users do not possess enough knowledge to understand it and thus, decide about the veracity of the discourse. Since the thesis also concentrates on the cyber security, it is essential to point out the three grammars of discourse of securitization in Hansen and Nissenbaum's approach. In addition, this approach expands the scope of referent objects to for example society or individual's sense of security (Hansen, Nissenbaum, 2009, p. 1163) which will be obvious in the focus of the DHS and other actors.

2.2. Agenda-setting theory

Hansen and Nissenbaum's approach provides an explanation of the agenda-setting powers of the DHS and other actors by showing their interpretation of threats and cyber security discourse. To complement the approach, the thesis employs some agenda-setting theory elements. The theory dates back to 1970s as an approach attempting to explain to what degree media affects public opinion (Van Aelst., Walgrave, 2006, p. 88-89). In 1972, Max McCombs and Donald Shaw (1972) did research on the 1968 presidential election in Chapel Hill, by asking voters in the town about the most important political questions of the time and comparing it to their coverage in the media. Therefore, according to the theory, the media has the ability to indirectly influence public opinion

by covering chosen topics (McCombs, 1978). In political science, the theory is applicable in a different way where one political actor's agenda may be under the influence of another political actor (Van Aelst, Walgrave, 2006, p. 89). In practice, it means that the agenda of the parliament may shape the agenda of president and vice versa. The same logic could then be applied to the DHS where its agenda may shape the national cyber security strategy. Moreover, there have been studies showing that media coverage can also frame certain issues in a particular way, thus, further affecting the different actors (including policy makers) and their respective behavior (Hilgartner, Bosh, 1988). In the case of the DHS, the issues covered by this federal agency, thus may be framed in an exceptional manner, and affect other actors. Different media use different methods to achieve this goal.

There are three types of agenda-setting: public agenda setting, media agenda setting, and policy agenda setting (Dearing, Rogers, 1996). For the purpose of this thesis, the focus is on the policy agenda setting. In general, just as the media can shape the public opinion, policymakers are just as, or even more, influential than them (Cobb, Elder, 1971, p. 903, 908-909). The topics covered by media may need backing by at least one decision maker (they are considered to be the guardians of the formal agenda) in order to become important on the agenda (ibid, p. 907). Moreover, decision makers' preferences, affiliation to particular groups and political parties, and the significance of certain groups further affect the topic's position (ibid, p. 908-909). In the adapted approach in this thesis, it would mean that the DHS may possess the power to shape the public opinion, yet to push certain agenda, it might need backing of policymakers. The importance of the agenda depends on the previously mentioned factors influencing the policymakers. Therefore, since the theory can be adapted to political bodies, the thesis uses it in its advantage, and applies it to the DHS. It further suggests that this particular federal department may project its own agenda onto other actors as well as national policy.

The Hansen and Nissenbaum's approach provides an explanation of agenda-setting powers by demonstrating an interpretation of threats by the DHS and other actors in the area of cyber security. Yet, it does not concentrate on how the securitizing actors can push their agenda onto different actors or even national strategy. By adding elements of agenda-setting theory, the modified approach allows for the explanation of such actions, and uncover the power that securitizing actors hold. Moreover, it demonstrates how one governmental body can affect others.

The next part presents key concepts, which are later used in the thesis. This allows for the better understanding and delineation for terms, and clarifies the importance and problematic nature surrounding the topic. First, it describes what cyberspace is, and then it moves onto the cyber security and its main tenets.

2.3. Cyberspace

Cyberspace is a concept that was first coined by novelist William Gibson in the 1980s in his book Neuromancer (Eriksson, Giacomello, 2007, p. 4). In its early days, it could be simply described as a network of information technology ran by its users. However, as the time went by and the technology advanced, a number of more complex definitions appeared. More specifically, with the discovery of the Internet and its TCP/IP (Transmission Control Protocol and Internet Protocols), the network became interconnected, and gained a completely new significance. The open architecture of the Internet allows anyone to use its tools, no matter what their intentions are. This principle is called the net neutrality, described by Tim Wu as: '*an Internet that does not favor one application over others (*Wu, cited in Glen, 2014, p. 644).' Moreover, there are many different definitions of cyberspace from various authors and institutions. For instance, the DHS perceives cyberspace as '*as the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries. Common usage of the term also refers to the virtual environment of information and interactions between people* (The White House, 2009).' Just as there are complex definitions, there are also broader ones: '*the information space consisting of the sum total of all computer networks* (Denning, 1999).' While some authors perceive it as a whole new domain with its own rules: '*... cyberspace is a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies* (Kuehl, 2009, p. 28).' As it was demonstrated, there is not a consensus on a unified definition of cyberspace. The focus of the descriptions varies from simple interconnected networks, complex systems in critical industries, to a new domain with a specific nature. It could indicate the need of agenda-setting in the framing game of cyberspace since it may help unify and solidify certain definitions, and also explain how certain actors adapt their perceptions of it.

Furthermore, cyberspace is a complex area filled with many different actors from NGOs, individuals, to states. Especially the military and the state are highly vested in the area and are arrogating competencies. There are contradictory elements between the borderless and fluid nature of cyberspace and state policies trying to secure it. With the rise of cyber threats, states became increasingly interested in it, trying to create norms and regulations in order to protect themselves and their citizens. In addition, the capabilities of state and military, and non-state actors differ significantly. While non-state actors mainly focus on the use of protective measures against threats, military and state capabilities also include intelligence, surveillance or control of forces and operations (Kuehl, 2009). In general, it entails all information and communication technologies (ICT). On the one hand, cyberspace increased interconnectedness, simplified access to information, transactions, business, etc. On the other hand, just as it brought benefits, the threats started to arise. The properties of the internet allow the perpetrators to work undetectably so they are never found, their origin is unknown, and it is difficult to prove who did what. For these reasons, many authors point at the correlation between cyberspace and the military which has been interested in its uses for some time (see also Cavelty, 2013; Barnard-Wills, Ashenden, 2012). Cyberspace is also often described as the fifth domain of military operations, in addition to aerospace, land, outer space, and sea (Kuehl, 2009, p. 27-28). This link results in the use of a military related vocabulary within the context of cyberspace such as cyber threat, cyberterrorism, cyberattack, cyber war, cyber warfare etc. (Barnard-Wills, Ashenden, 2012). It culminates into the negative and dangerous perception of cyberspace, which could be misleading and damaging. This perception of cyberspace potentially allows the DHS to use this discourse for its advantage by stressing the need for additional protection.

2.4. Cyber security

Cyber security has been a progressive academic, political and security area that has been gradually gaining importance since the early days of cyberspace. The threats of cyberspace have been already known since 1970s. Yet, when the first impactful computer bug called Y2K hit, cyber security became much more significant (Eriksson, 2001, p. 218). Then, after 9/11 there has been a spike in the protection of cyberspace, which led to the development of new security policies in many states. As it could be observed in the case of cyberspace, cyber security does not have a unified definition of what it entails or what it is either. In its basic form, cybersecurity could be

translated as a protection of cyberspace. Yet, there are more things that need to be included. For example, the DHS stresses the importance of cyber security as it observes '*there is 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* (DHS, n.d.w).' Another often used definition was introduced by the International Telecommunications Union (ITU): '*the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets* (International Telecommunication Union, n.d.).*'* The European Commission shares similar views as the ones of the DHS, as it sees cyber security as '*the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military field, from those threats that are associated with or that may harm its interdependent networks and information infrastructure* (European Commission, 2013).' Noticeably, there is not a consensus on the definition of cyber security. Yet, a trend can be identified among scholars and institutions. It could be said that there is a general agreement about a security concern in cyberspace that needs to be tackled, although, it does not state where the threats appear, or what they essentially are. This can also help the DHS with pushing their own agenda on the national strategy since there are not clear definitions of threats in cyberspace. As a federal body that deals with large number of cyber security related operations, it can bend the meaning of threats in a way to suit its needs, and help it to set the discourse.

To conclude, the securitization theory is used to evaluate the discourse in the official documents released by the DHS and other officials, as well as the discourse in the documents the DHS has worked on. It demonstrates how this federal department sets the discursive and political agenda, and how it frames the U.S. national cyber security strategy under its influence. In order to do that, the thesis applies political discourse analysis, which reveals the constitutive effects on politics and national strategy (Campbell, 1992). The main source of data comes from the official documents released by the DHS, the White House, and other federal agencies and departments. Other sources include scientific articles, periodic journals, books, news articles, as well as official webpages of related actors (The White House, the DHS, etc.). The time frame is limited by the Reagan administration onwards, and with 9/11 as a focal point. Additionally, it looks for three grammars of securitization outlined in Hansen and Nissenbaum's approach, namely hypersecuritization, technification, and everyday security practice. To do that, the thesis utilizes

an analytical software – Atlas.ti - for qualitative discourse analysis which searches for terms related to these grammars such as military, national security, security etc. It brings to light if the DHS and other officials aim at securitizing cyberspace, and the perception of the cyber security in the U.S. Furthermore, the thesis shows the agenda-setting elements, which further clarify the agenda-setting power of the DHS as an influential player in the area of cyber security on national strategy.

Moreover, the thesis analyzes the contextual circumstances under which the DHS was founded, the powers it was given in the field of cyber security, as well as its specific position among federal agencies, which may uncover its influential impact on the U.S. national cyber security strategy. To demonstrate the complex network that the agency possesses in the area of cyber security, the internal cyberspace branches of the agency are presented. The historical analysis aims at uncovering trajectories and ruptures in the cyber security field in order to provide a better perception of the evolution of the U.S. cyber security strategy. In addition, the thesis utilizes process-tracing to clarify the temporal processes leading to transformations in the discursive and institutional frameworks in the U.S. cyber security field. These methodological approaches as well as discourse analysis will be presented in the next chapter to illustrate the analytical processes used in the thesis, and how it will proceed.

3. Methodology

This chapter presents the analytical approaches, which are applied in the thesis, including political discourse analysis, historical analysis and process tracing. These different qualitative methods of analysis facilitate a better triangulation of data through cross verification from multiple sources and by applying a combination of several research methods during the research. In this regard, the discourse analysis helps with the identification of the securitization discourse, and therefore either confirms or disproves whether the DHS participates in the securitization of cyberspace. Furthermore, historical analysis and process tracing allow for a better understanding of the context of the securitization, as well as the historical origins and structural conditions of the particular stance towards cyber security in the U.S.

3.1. Discourse Analysis

The thesis concentrates on several topics. The first one focuses on the cyber security discourse in the U.S., more specifically the discourse issued by the DHS. Discourse can be perceived as a set of ideas, concepts, or a particular way of conversation that gives meaning to social and physical phenomena, which are produced with the use of specific sets of practices (Hajer, Versteeg, 2005, p. 175; Van Dijk, 2011, p. 2). Moreover, discourse could be seen a form of language use (Van Dijk, 2011, p. 2) which may imply that the discourse analysis could then be simply defined as a study of language (Johnstone, 2018, p. 2). In this case, the language does not only embody verbal communication but it further includes written language, communication and interaction (Van Dijk, 2011, p. 3). In addition, some authors also use images, videos and other visual tools as part of the language (Wang, 2014; Frohmann, 1992; Amirian, Rahimi, Sami, 2012). According to the theory, language shapes one's view of the world while it also allows to see how different actors try to influence the definition of a certain issue (Hajer, Versteeg, 2005, p. 176-177; Jorgensen, Phillips, 2002, p. 18-19). This may be visible in the case of the DHS and its approach to cyber security strategy, which might be influencing the national cyber security strategy, thus, even the perception of the cyber security as a field of study in the U.S. Moreover, discourse analysis can be either interpretative or social constructivist, which means that it sees the reality as socially constructed while stressing the existence of multiplicity of these realities that are governed by natural laws (Hajer, Versteeg, 2005, p. 176).

Discourse analysis presents a multi-theoretical constructivist approach that perceives the understanding of the world as a creation of social processes preventing it to be seen as objective (Jorgensen, Phillips, 2002, p. 5-6). Therefore, reality is also perceived as a social construct, and thus, is not predetermined. Furthermore, it is an approach that links discourse and context together to reveal how certain social constructions are brought to life and what their purpose is (ibid, p. 6). There are different approaches to discourse analysis, which use different theories of grammar and lead us to different explanations of the meaning of the discourse (Gee, 2004, p. 8).

However, discourse analysis faces several problems. First, there is a problem with the form of the written data that discourse analysis is dealing with, because it presents a product of a verbal act rather than interaction. In this case, the discourse has to be perceived as both – talk and text. Second, the word discourse can imply many things, which may stir confusion. In order to resolve that, the word itself may be completely avoided by some analysts. Moreover, there might be complications with delineating the discourse, which of course comes with close analysis of an outlined issue. Then, there is a need for the distinction between different concepts, discourses etc. used in the analysis (Van Dijk, 2011, p. 2-5).

3.2. Political Discourse Analysis

The thesis specifically employs political discourse analysis because of its focus on political discourse. Political discourse analysis enhances critical discourse analysis since it concentrates on the political discourse while also being critical. Moreover, one of the advantages of the critical-political discourse analysis for this thesis is that it deals with for example the reproduction of power, or domination with the use of political discourse (Van Dijk, 1997, p. 11). The discourse is identified through its actors – politicians or political actors. Yet the actors, who are being elected and paid for their political activities, may not be the only players in the discourse. Based on the context it further includes the recipients of the discourse such as the public (ibid, p. 12-14). For the purpose of this thesis, the actors will be delineated to those participating in political actions including governing, ruling, legislating, influencing political decisions etc. Political discourse can be called political only if it is functional within the debate, 'for the record', and if it contributes to the topic discussed (ibid, p. 20). Moreover, it should be part of the political process in some way. Additionally, if the political talk is so-called 'off the record', and later is printed in the media, it may have some political function (ibid, p. 21).

Political discourse can be differentiated from societal discourse by several factors, although it does not always have to be fulfilled. Furthermore, these factors should not be taken as absolute because the context should also be taken into account. The 'official language' is discursively, politically and legally mandatory (ibid, p. 24). In general, there is no restriction between the topics that can be part of the political discourse but there is a limitation on the topical participants that can contribute to the political process – public actors. The macrostructures of the political discourse are often future-oriented such the threats, promises, future development etc. Topics may include evaluations, and will often be about political actors and their typical actions (ibid, p. 27-28).

Compared to the classical discourse analysis, political discourse has a higher level of complexity because it needs a political explanation and context such as norms or ideologies. In addition, public reaction, and political economy could be taken into account. Therefore, political discourse analysis offers an insight into discursive political practices, which require their own analysis of the structures, influences, effects, etc. It further allows for better understanding of political practices, their context and the effects they have on the public. Moreover, it explains the discursive processes of agenda setting, and the relations between politics, media and public opinion (ibid, p. 40-44).

However, political discourse analysis does not provide a clear methodological approach. Because it is an extension of the critical discourse analysis, the thesis uses its analytical framework, more specifically Norman Fairclough's discourse approach. Critical discourse analysis has a long tradition since the 1980s. As it became more popular, it expanded into a wide variety of different approaches towards social analysis discourse (Fairclough, 2013, p. 24). The research outlines the analytical techniques that are relevant to it, as well as the basic presumptions of the theory. According to Fairclough, it is a transdisciplinary approach defined as 'the theoretical and methodological development' (the latter including development of methods of analysis) of CDA and the disciplines/theories. Additionally, the development is in dialogue, through which it is informed, and is a matter of working with (though not at all simply appropriating) the 'logic' and categories of the other in developing one's own theory and methodology.' 'It is used to identify linguistic, semiotic and interdiscursive features of the text (Fairclough, 2001, p. 2).' Social events are made out of two causal powers – social practices, and social agents (Fairclough, 2003, p. 23-24). Analysis of the texts includes interdiscursive analysis (how genres, discourse and styles

articulated together) which allows for a better understanding of context, linguistic analysis, and semiotic analysis (for example visuals) (Fairclough, 2003, p. 37-38). Moreover, Fairclough works with a term 'discursive event', which is defined as an event which can at the same time present a piece of text, an instance, an instance of discursive and social practice. This combination adds the explanatory value to these events because they entail more information from different perspectives (Fairclough, 1992, p. 3). Furthermore, different discourses can represent how things were, are, or should have been. They can be either materialized, enacted or inculcated which depends on them being turned into successful strategies (Fairclough, 2003, p. 207-209).

In the methodological sense, critical discourse analysis presents a detailed textual analysis where the data chosen depends on the project and object of research (Fairclough, 2013, p. 185). It closely evaluates opaque and transparent structural relations of control, discrimination, dominance and power, which appear in language (Weiss, Wodak, 2007, p. 15). Moreover, the method requires an analysis of the intertextual interplay of discourses and their relations with one another. In addition, it is also crucial to place these discourses in retrospect in order to be able to make coherent arguments and explain the contexts, genres, strategies, localities, etc. Simply put, the analysis looks for the relations between the language, the context in which it takes place, as well as how it is used, and what influence it has (Fairclough, 2003, p. 35-38). From this point of view Fairclough's CDA is a useful tool to identify the rhetoric appearing within the documents by the DHS because in the case of this federal department, the events surrounding its establishment need to be taken into account, as well as historical relation of this actor with cyber security. Additionally, since multiple documents are examined, the discourse interplay play an important role in the thesis. Moreover, the same can be applied to the analysis of the National Cybersecurity Strategy of the United States of America, where the context can pose as a crucial element to the discourse within the strategy. The research encompasses the combination of semiotic and non-semiotic elements and looks for the relation between them. Moreover, the analysis stresses the importance of highlighting the context which is necessary for understanding a certain discourse (ibid, p. 12-13, p. 52-53).

Fairclough's approach links to Gramsci's concept of hegemony and power, which leads to the use of the discourse as a process of forming, negotiating power relations and ideological processes rather than the use of language. His approach can be linked to the thesis which intends to look for the power of the DHS, the securitizing discourse within its documents relating to cyber security, and its possible effects on the national cyber security strategy of the U.S. Since the

strategy has been developed by the president and the National Security Council, the DHS may have pushed its own agenda and rhetoric onto these actors which then transferred it into this document. Thus, this approach helps of CDA may help uncover the hidden relations between the actors, and explain what could be the consequences. Therefore, a certain discourse is connected to a particular ideology, which embodies knowledge, beliefs, as well as positions of social actors (Fairclough, 2001, p. 93-94).

The analysis is done at three levels – text, discourse practice and sociocultural practice. At the same time, it is a theoretical combination of Gramsci's concept of hegemony and intertextuality (Fairclough, 2001, p. 133). First, the text is analyzed through the linguistic analysis, which looks at grammar, semantics, sound system, vocabulary, etc. in order to highlight the interdependency. It also describes the genres and styles within the text (Fairclough, 1995, p. 57; Fairclough, 2001, p. 133). Furthermore, Fairclough stresses that this analysis helps search for three elements within the text related to it – identities (between the writer and the reader – personal and social), relations (mainly between the writer and the reader) and representations (it involves recontextualizations and representations of social practices) (Fairclough, 1995, p. 58). Therefore, it includes the description of the text itself, as well as its connection to other discourses. Because the thesis works with different discourses by various actors, making the connection is a crucial step for understanding the whole analysis, as well as uniting the entire research.

Second, according to Fairclough, the discourse practice combines society and culture on one hand, and the language and text on the other (Fairclough, 2001, p. 10). According to Fairclough, this level further encompasses processes of text production, distribution and consumption, as well as sociocognitive aspects (Fairclough, 2001, p. 2, 134). Compared to the first level, this one includes the analysis of actors' interpretation of the events, and how it further influences the texts, as well as the relation between discourses and the actors involved. Moreover, it also examines the power relations, and how the superior discourses and actors push their own beliefs, etc. onto others (Faiclough, 1995, p. 60-61). Interdiscursivity shows how texts are a combination of various genres and discourses while also demonstrating a historical view of text and their transformation from past to present (Fairclough, 2001, p. 134). It is especially useful for the agenda-setting part of the thesis which concentrates on the DHS's power to push its own agenda onto the national strategy. It can further compliment the historical analysis and process tracing which also try to answer this question.

Lastly, the sociocultural practice focuses on the explanation of the context (political, historical, situational, etc.) and other factors affecting the production, transformation, acceptance of the text itself. There are generally three aspects of the sociocultural context: cultural, economic and political. This can help uncover causal mechanisms hidden in the discourse. Additionally, Fairclough stresses the fact that not all levels of analysis have to be performed but they might uncover information, which allows for a better understanding of a particular event (Fairclough, 1995, p. 62; Fairclough, 2001, p. 87-90, 97). Furthermore, the genres and discourses are limited by the hegemonic relations and struggles (Fairclough, 2001, p. 134). Yet again, this level compliments the historical analysis by adding a level concerned with the context surrounding the texts, which allows for a better understanding of the steps that led to the creation of particular documents or discourses. On top of that, it enhances the process tracing method since it also covers the causal mechanisms but from a different perspective hidden in the discourse itself.

By utilizing the political and critical discourse analysis, the thesis is able to demonstrate the influence of political actors on national strategy and politics. Furthermore, it helps reveal whether or not the DHS and other government officials attempt to securitize the cyber security in the U.S., and its overall perception. This analytical technique is better suited than the classical discourse analysis because it focuses specifically on the discourse that is occurring in the thesis, and therefore can more thoroughly explain the discursive intricacies related to cybersecurity. Furthermore, since it also considers context to be a crucial part of the analysis, it allows, yet again, for enhanced evaluation of the texts, speeches and other sources. In the case of the DHS, it applies to the situation surrounding its creation, as well as its reorganization, and other significant events. The same applies to other actors that have tried or try to influence cyber security discourse in the U.S. Lastly, its emphasis on agenda-setting corresponds to the focus of the thesis which also tries to reveal whether the DHS has the power to push its own agenda onto the national cyber security strategy, and influence the image of cyberspace in general.

3.3. Historical Analysis

Historical analysis is a qualitative type of analysis that is usually and ideally used on a single cases or a small number of cases. In international relations, the analysis is used for description and explanation of historical events. It stresses the importance of the choice of primary and secondary literature in order to avoid bias and selectivity (Thies, 2002, p. 352-366). The thesis

briefly applies this analytical framework starting from 9/11 that is perceived as an exogenous shock triggering a sequence of events, including the creation of the DHS, as well as the crystallization of the U.S. cyber security strategy, its possible securitization which has affected it for the years to come. It aims at reconstructing trajectories and possible ruptures in the cyber security field and to provide a more comprehensive image of the evolution of the U.S. cyber security strategy. It provides the thesis with analysis of the historical events such as 9/11, which are crucial for understanding the historical context of the actions that followed. Moreover, it helps with the introduction of the problematics, as well as the basis of the broader popular perception of cyber security in the U.S.

3.4. Process Tracing

Process tracing is a tool of qualitative analysis that is defined as 'the systematic examination of diagnostic evidence selected and analyzed in light of research questions and hypotheses posed by the investigator (Collier, 2011, p. 823).' It can help explain causal claims of political and social phenomena. It can contribute to a description, evaluation, of social and political phenomena, as well as gaining insight into causal mechanisms, and providing alternative explanations. In order to identify causal mechanisms, diagnostic evidence needs to be found. Process tracing looks at how events evolved over time (Collier, 2011, p. 823-824). It further involves searching for observable implications of hypothesized explanations to decide if the situations unfolded as it was predicted by alternative explanations. The contribution of the evidence to alternative hypothesis is more important than the amount of data. In general, there are four main tests that lead to either confirmation or rejection of explanations with the use of evidence with different probative value (Bennett, 2010, p. 2-4). The tests are Straw-in-the-wind, Smoking Gun, Hoop Test, and Double Decisive Test. Firstly, the Straw-in-the-wind is not decisive by itself and it does not provide necessary nor sufficient criterion for acceptance or rejection. Secondly, the Hoop Test does not by itself confirm the hypothesis but in the case of rejection, it eliminates it. Thirdly, the Smoking-Gun Test offers a sufficient but not necessary criterion for acceptance of the hypothesis while failing the test does not eliminate it. Lastly, the Doubly Decisive Tests leads either to the confirmation of the hypothesis while eliminating all the other alternatives, and the failing of the tests results in the rejection of the hypothesis (Collier, 2011, p. 825-827). The Smoking-Gun test is later used in thesis to identify whether there was a securitization of

cyberspace, and cyber security after the 9/11 in the U.S., and if this event served as a catalyst to this step. It is crucial for identifying the rhetoric of the DHS in this area, and serves as a base for the following chapters.

The thesis employs this analytical method to investigate and explain the temporal, ideational and material processes, which led to significant transformations in the discursive and institutional frameworks in the U.S. cyber security field. It is the best approach to trace the causal claims of the events that unfolded in the U.S. because it looks at alternative perceptions of the events, which may be crucial for understanding the current situation in the field. Moreover, it can uncover additional factors that influenced the national cyber security strategy by describing and evaluating the moves made by the DHS and other government officials interested in the field.

All of the mentioned methodological approaches help with an explanation of the situation surrounding the cyber security field in the U.S., as well as the position of the federal agencies in this area. Additionally, it provides a look at the evolution of the cyber security in the U.S., and the perception of it. Moreover, it further uncovers the standing of the DHS in this field, the agenda-setting power it possesses, and the extensive cyber security network within it.

3.5. Operationalization

The thesis concentrates on the analysis of the U.S. cyber security policy, and the assessment of the agenda-setting power of federal agencies in this field, specifically the DHS. The DHS was chosen as a case study because it deals with a significant number of cyber related tasks in the U.S. while also being tasked with the provision of national security, which gives it a central position as an agenda-setter in other security-related areas. Furthermore, it attempts to explain why there have been efforts to securitize the area of cyber security, although there is an inconsistent stance towards it in the U.S. among policymakers, as well as scholars. Moreover, several discursive events that include mainly the DHS as a securitizing actor are analyzed, as well as other government officials such as the President of the U.S. Thus, the research questions are: What is the cyber security strategy of the U.S.? Has there been a securitization of cyber security after 9/11? And is the DHS successfully setting the cyber security agenda on the national level?

What connects the academic articles, news articles, interviews, etc. is the concentration on the topic of cyber security. The main analytical technique used to operationalize the data, is the political discourse analysis which helps uncover common patterns in the discourse that is shared

throughout the different texts and documents. Moreover, it utilizes the modified securitization theory by Hansen and Nissenbaum in order to reveal the possible securitization of cyber security discourse in the documents of the DHS and the discourse of government officials. It is approached by searching for three elements of securitization of cyberspace: hypersecuritization, technification, and everyday security practice. In order to do that, the thesis uses the methodological approach by Norman Fairclough. The three level analysis, including text, discourse practice and sociocultural practice in a way best suited for the chosen topic of the research. It is applied to the documents by the DHS and government officials, news articles, interviews and speeches. To identify the securitizing discourse, the thesis a qualitative analysis computer software: Atlas.ti which is able to create codes to categorize data and find relations between words, or make word count. It facilitates the process of discourse analysis, and can demonstrate the hidden rhetoric in the documents.

The historical analysis does not exactly prescribe a method how to approach the analysis. In the thesis, it is used to map 9/11 and the events post 9/11 related to cyber security field in the U.S. Therefore, the analysis is limited by the year 2001 forward. It also includes the historical analysis of the establishment of the DHS, which is then used in a later chapter to explain its stance towards cyber security. In addition, this kind of analytical technique provides a historical background necessary for the understanding of the topic. In combination with process tracing which has been presented as an approach allowing for explanation of causal mechanism, and alternative interpretations it may help not only demonstrate the changes in the U.S. cyber security field but also examine why they occurred in the first place. In order to utilize process tracing, the Smoking Gun test described in the methodological chapter is employed to either confirm or deny the outlined alternative explanations, which may further lead to the discovery of causal mechanisms.

The first step of the analysis describes and explains the historical, political, and social context of 9/11 onwards which sets up a base for a wider understanding of the events that unfolded, while also providing the context that is described in the securitization framework (Balzaq, Léonard, Ruzicka, 2016). Furthermore, it provides a better image of the evolution of the U.S. cyber security strategy. Additionally, the step also includes searching for causal mechanisms that led to a transformation in the cyber security in the U.S. after 9/11 by using the process tracing test on the alternative explanations laid out in the chapter. Thus, first the alternative explanations are outlined, and later are put into test in relation with the historical analysis. It also helps explain whether the

DHS possesses the agenda-setting power to push its own agenda onto the national strategy in cyber security.

The second step involves the choice of the relevant written sources, which are categorized based on the actor that it relates to. All the actors in the thesis have a connection between each other, yet the distinction is important to highlight the possible power they possess in the area of cyber security. Each of the written discourses is then analyzed using the Fairclough's three level analysis modified to properly capture the topic. The thesis also examines the intertextuality and interdiscursivity among the texts which uncovers a connection between them. First, texts are analyzed by themselves through the linguistic analysis which looks for identities, relations and representations, as well as Hansen and Nissenbaum's hypersecuritization, technification and every day security practice. Then, the relations between actors, discourses are examined, as well as the interpretations of the events from the perspective of the actors. Lastly, the wider political, historical, and social context is yet again brought to light to help uncover possible new causal mechanisms in the discourse. It may show the influence of certain actors on the national strategy and politics in the area of cyber security in the U.S., as well as the possible securitization of the discourse in the cyber security field. Furthermore, it also demonstrates whether or not the DHS has the agenda-setting power in the area of cyber security on the national level.

Lastly, the analysis closely examines the DHS as an agency involved in the cyber security area and provides a description of its branches involved in this field. Furthermore, the agenda-setting power of the DHS is examined, as well as its influence on the cyber security national strategy in the U.S. It then summarizes the results from the previous steps, in order to answer the outlined research questions. The last part provides concluding remarks.

The next chapter presents the historical analysis of the establishment of the DHS, approach to the cyber security since the Reagan administration, as well as the evolution of the cyber security within each of the administration post 9/11. It also demonstrates the effects of this events on this field, and this federal department, while also employing the process tracing Smoking Gun test to decide if there has been a securitization of cyberspace after 9/11.

4. Historical analysis

This chapter provides a historical analysis of the events that preceded the foundation of the DHS, such as 9/11 terrorist attacks. This moment signifies an exogenous shock to the U.S., as well as an important juncture in time that triggered the establishment of the institution itself, allowing for a complex understanding of the context that shaped its following actions, and its latter approach to cyber security. Additionally, the chapter further presents the basis of the perception of cyberspace and cyber security in the U.S., and the way the events of 9/11 impacted this field. It is important to include the historical analysis of the events preceding the establishment of the DHS in order to better understand its approach to tackling problems, and its latter expansion in the cyber security area. It also uncovers its enhanced powers in the agenda-setting onto the national cyber security strategy, and where it originated. Likewise, the evolution of perception of cyber security offers a complex outlook on the securitization that could have taken place in this field. After presenting the events up to the Bush administration, the process tracing test takes place to decide whether the securitization occurred after 9/11 or not.

4.1. Cyber security and the DHS before 9/11

The ideas for the establishment of the DHS preceded the events of 9/11. Before that, its activities were spread among 40 federal institutions. The first major draft appeared in 1998 when Mac Thornberry proposed a bill that would create a sole institution for national security, but the proposal did not go through. Then, however, on 9 September 2001, the tragedy struck the U.S. when the terrorist attacks in New York happened (Borja, 2008, p. 3-4). On September 22, 2001, President George W. Bush pledged to create an office of Homeland Security in the White house that would tackle the national strategy in the fight against terrorism, and further prevent and respond to future attacks. The moment of October 8, 2001, followed with the establishment of two institutions within the White House – The Office of Homeland Security, which was directly part of the Executive Office of the President and tasked with the creation and implementation of national strategy; and the Homeland Security Council (HSC) composed of cabinet members, advising the president about national security agenda (ibid, p. 4). Part of the HSC was the Office of Cyberdefense which worked on the national security strategy of the U.S. (Cavelty, 2008, p. 26). After the release of a document called Critical Infrastructure Protection in the Information Age, the powers of the national coordinators expanded to responsibilities including the virtual and the

physical security of critical infrastructure (ibid, p. 26-27). On October 26, 2001, the Congress passed a Public Law entitled The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, otherwise referred to as USA PATRIOT act. It increased the capabilities and authority of the government agencies to tackle terrorism including the Electronic Crime Task Force which was tasked to help uncover crimes supporting terrorist activities and their funding (United States, 2001). Later, on March 21, 2002, the number of institutions was expanded by the establishment of the President's Homeland Security Advisory Council that consisted of advisors from public and private sector, giving their insight on homeland security matters (Borja, 2008, p. 4).

However, the efforts to create the all-encompassing institution fully uncovered in February, 2002, when George W. Bush presented a budget proposal that included various support for areas of homeland security such as border security or technology. On June 6, 2002, George W. Bush proposed the establishment of a permanent institution - the Department of Homeland Security - that would be tasked with the national strategy, while also outlining its four main divisions – Border and Transportation Security; Emergency Preparedness and Response; Chemical, Biological, Radiological, and Nuclear Countermeasures; and Information Analysis and Infrastructure protection. This was followed by a legislative proposal that ultimately led to a creation of a Transition Planning Office which was supposed to coordinate the whole establishment of the DHS (Borja, 2008, p. 5-6). The first National Strategy for Homeland Security was released in July, 2002, and set three objectives for the newly emerging institution – preventing terrorist attacks within the U.S., reducing its vulnerability to terrorism, and minimizing the damages and recovering from attacks. Finally, on November 25, 2002, the Homeland Security Act of 2002 established the Department of Homeland Security (ibid, p. 7-9). The DHS combined 22 separate departments and agencies (Kaiser, 2005, p. 8). One of the agencies was the Federal Emergency Management Agency (FEMA) which was supposed to serve as a responder to major tragic events while also expanding the tasks of the DHS as an institution (Borja, 2008, p. 5).

The evolution of the DHS shows that although previous proposals were made to establish an encompassing homeland security agency, the 9/11 events acted as a significant catalyst to implement such ideas into practice. They also provide an important source of legitimation and urgency to justify the rationale behind the creation of such an institution. Furthermore, the encompassing nature of the DHS meant that by combining different departments and agencies, it

gained reach to various areas, one of those also being cyber security. Furthermore, it then allowed for an easier enlargement into new sectors, and an extension of its powers and influence as it will be demonstrated in the upcoming chapter. This is significant for this thesis in several ways. First of all, it points at the specific environment surrounding the establishment of the department, and the need for a resonating event that would allow it. It could have also paved the way, the DHS treats and approaches its given tasks even in the area of cyber security.

Cyber security in the U.S. has a different story. There have been multiple bills, plans and proposals to regulate cyberspace in the past. Furthermore, as the time went by, the institutions involved in this area have expanded as the fear of its potential damages evolved. The first efforts could be seen during the Reagan administration which was afraid about its possible damaging effects by exploiting classified information. However, the first document to explicitly mention the threats of cyberspace was the National Security Decision Directive Number 145 (NSDD-145) on National Policy on Telecommunications and Automated Information Systems Security, issued on September 17, 1984 (The White House, 1984). It even included the notion about the fact that it is 'used extensively' by terrorists or criminals. Thus, there could be seen first efforts to put a certain 'label' on cyberspace as a tool used by terrorists and criminals. Likewise, the perception of cyberspace was shifting with the changes within the military, especially the Revolution in Military Affairs (RMA). In general, it means the application of new technologies for military advantage that led to a significantly increased budget for research and development programs in the U.S. The U.S. realized the potential of quickly growing field of technologies and cyberspace, but it also brought fears about the technological race with the adversaries which could lead to the undermined position of the U.S. in the international arena.

Moreover, in a way, it implied the militarization of space and cyberspace, while also increasing the budget for DoD IT security programs (Kundnani, 2004, p. 119-120). Despite the fact that there is a disagreement about the beginning of the RMA, it could be argued it was mainly tied to the exponentially growing importance of cyberspace in the 90s (Lindsay, 2014). The technological superiority of the U.S., however, made the state paranoid since it started to fear possible data breaches after the Gulf War where its technological and communication dominance played an important role (Cavelty, 2008, p. 24-25). This was further emphasized after the 1995 Oklahoma City terrorist attacks, which led to an ultimate realization that the untraceable nature of cyber-attacks, allowed the perpetrators to operate unknowingly. For these reasons, the Clinton

administration started developing cyber security national strategy called Presidential Commission on Critical Infrastructure Protection (PCCIP) in 1996. The commission focused on the cyber related threats which could expose vulnerabilities of the U.S. critical infrastructure (Federation of American Scientists, 1997). When it finally released a report in the 1997, it emphasized the topic of cyber threats and the need for critical infrastructure protection, and it ultimately led to an adoption of the protection against them. The commission pointed at the growing danger of cyber-attacks that needed to be addressed by the government (Federation of American Scientists, 1997, p. 14). Furthermore, it created a new terminology including terms such as cyber-terrorism or the electronic Pearl Harbor (Cavelty, 2008, p. 26). This points at an interesting reality that the framing of cyberspace as a potential threat already widely appeared in the 90s, and it also hints towards unpredictable military strikes and militarization tendencies. However, the capabilities provided by cyberspace at the time were not as big as they can be today, the fear of its use by terrorists was significant. In addition, the terminology that was invented in the PCCIP framed one of the most possibly devastating cyber-related incidents without any similar, or bigger cyber events of this kind at the time. This may mean that the first attempts to securitize cyberspace could be traced to this document which tried to threat frame it as an imminent danger. It then paved a way for an easier acceptance of cyber security, and cyberspace as a tool for crime and terrorism because it was emphasized since the 90s, and 9/11 only provided an opportunity to fully securitize it.

The attacks of 9/11 were the deadliest terrorist attack on American soil resulting in roughly 3000 deaths. After the events, one of the priorities was an improvement of interagency coordination, since it suggested a possibility of a future occurrence (Kaiser, 2005, p. 2; Perrow, 2006, p. 1). The tragedy allowed for the securitization of various sectors in several ways. First of all, the shock of the event was multiplied by the fact that the U.S. was unprepared for such an event. After the fall of the Soviet Union, there was no apparent enemy in the traditional sense of state-to-state combat where an enemy is known, which created a threat deficit (Perrow, 2006, p. 2). With the RMA, the U.S. adversaries started emerging in the technological race where they could endanger U.S. position as a technological superpower. The cyber domain opened up a way for new kind of attacks that were untraceable, potentially easily executable, and could hit from any place on the planet with their unlimited reach. Likewise, the proliferation of non-state actors started to surface, yet before 9/11 it was not as emphasized as after the events when it was mainly tied to terrorists (Russell, 2006, p. 645). However, the U.S. was not prepared for an attack of this kind.

As it could be seen, it was focusing on threats of a different nature. Moreover, the gruesome devastation of the events was repeatedly emphasized, systematically publicized and extensively broadcasted. This served the purpose to engrave into people's minds that anyone, anywhere can become a victim of such attacks. Moreover, it further led to fear within the U.S. government that the country is vulnerable. In the President's speech to both chambers of Congress on September 20, 2001, George W. Bush emphasized the uniqueness of the event, and the need for new means, and countermeasures because the current ones were not adequate to tackle a crisis of this scale. This implied the construction of a new kind of threat, as well as the creation of new emergency measures to tackle it, this being in line with typical signs of securitization moves (Mabee, 2007, p. 389-390).

Additionally, it allowed for the creation of new security institutions such as the DHS. Taken all this into account, the audience was easily convinced that terrorism presented a real threat. However, the audience did not only approve of seeing terrorism as a threat, but also other areas including cyber security. Cyber security was part of the expansion of the national security strategy of the U.S. which then slowly became perceived as one of the biggest threats to the nation. This may have created a link between the new threat environment, the securitizing discourse and cyber security. The fear of future attacks was further captured by the ongoing emphasis on repeating the events of 9/11, as well as the rhetoric of the governments and the U.S. President. Then of course, although, there were no major cyber-attack that would have been a danger to the country in the past, cyberspace became a possible tool for terrorists trying to take down the country. This could possibly explain why the securitization of this field happened without any events that could allow for its securitization, or even closely resembling disastrous scenarios of the so-called 'electronic Pearl Harbor'. This scenario resembles a massive scale cyberattack that would incapacitate the computational and communication capabilities of the U.S. (Wirtz, 2017, p. 758-759). Thus, for the securitization of cyberspace, there was no need for a historical precedent, which could be pointed to as a reference point, because it was linked to viable terrorist tools. The long-term perception of cyberspace as a potential danger was tied to the U.S. information and intelligence gathering and privacy, the overall paranoia stemming from the superiority of the U.S. in this area, as well as its inclusion within the protection of the critical infrastructure. It further allowed for the securitization of this field, and an easier acceptance by the audience which saw it also in this

context. Moreover, this demonstrates the importance of the context of the events for the securitization theory, since it helps uncover other influencing factors for the theoretical approach.

The role of the DHS was and is to 'develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats or attacks', while also being tasked with providing a public security (The White House, 2001). From the very beginning of its existence, the DHS was tasked with information analysis and infrastructure protection, which was later on expanded to cyber security and other areas of cyberspace. However, its initial role and goals reflect the way this institution treated and keeps treating cyber security. Because it was tasked with the protection of the homeland, it started treating cyberspace as a part of it, in the terms of perceiving it as a potential threat to the national security. This further led to the use of tools specifically related to the protection of national security, although, in certain cases (e.g. digital economy), other instruments would have been more suitable. On top of that, cyberspace and cyber security have been in a way already perceived as a potential danger prior to the events of 9/11 which could have been ultimately seen as the securitizing moment because it could have been pinpointed as a tool of terrorists. It amplified the fear that has been surrounding cyber security since the Reagan administration, and allowed the government officials to put it under the special measures without at the time any disastrous events relating to this field. All of this further affected the nature of the DHS as a federal department, as well as its approach to solutions of its given tasks.

4.2. Cyber security field and the DHS after 9/11

The previous section demonstrated the context of the DHS establishment, the perception of the cyber security preceding the attacks, as well as the effects of the events of September 11, 2001, not only in these two fields but also concerning changes in federal department and agencies. Moreover, it helped explain why the securitization of cyberspace and cyber security occurred under such specific circumstances without any past catastrophic events in these areas or during the 9/11, which is an uncommon phenomenon within the securitization theory. The following section traces the development of perception of cyberspace in order to demonstrate the temporal, ideational and material processes which transformed the discursive and institutional frameworks in the U.S. cyber security field. Furthermore, the focus is limited to the main events relating to cyberspace, cyber security, as well as the key changes connecting it with the DHS. The section

also presents the Bush administration, the Obama administration, the Trump administration, and their major policy changes within the cyber security. Additionally, some of the outlined documents will be later analyzed with the use of the political discourse analysis.

4.2.1. The Bush Administration

After the 9/11, most of the U.S. government agenda focused on the fight against terrorism, however, in 2003, the President George W. Bush introduced a document called The National Strategy to Secure Cyberspace which reacted to a growing importance of cyberspace, and its involvement in the protection of critical infrastructure (The White House, 2003, p.9). The paper confirms the previous chapter's explanation for the securitization of cyberspace which can be already seen in the summary of the document where it is said to be 'part of our overall effort to protect the Nation' (The White House, 2003, p. 7). It was marked as an area that needed protection because of the possibility of a threat, and the difficulties surrounding the establishment of security in cyberspace. It referred to various actors from private and public sector, but also the American people themselves to take action against the vulnerabilities within this area (ibid, p. 7-8). Its main strategic objectives stemmed from the National Strategy for Homeland Security and included: prevention of cyber-attacks against the U.S. critical infrastructure, reduction of national vulnerability to cyber-attacks, and minimization of damages and recovery time from cyber-attacks (ibid, p. 8). As a solution, it calls for various improvements such as the creation of the response systems, national strategies, cooperation between public and private sectors, sharing of information among intelligence agencies, or support of the DHS to coordinate crisis management for cybersecurity (ibid, p. 8-13).

In order to support the role of the DHS within cyberspace, at the end of the year 2003, President George W. Bush followed with the Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization and Protection (HSPD-7) (U.S. Government Publishing Office, 2008, p. 33). The main purpose of this directive was to improve the protection of the critical infrastructure against terrorist attacks (physical and cyber-based) by the federal departments, yet, it also included the enhanced security of cyberspace. It further expanded the role of the DHS in the area of protection of critical infrastructure to cyber related one. Moreover, it emphasized the importance of information sharing between the DHS, other federal departments and agencies, and private sector (U.S. Government Publishing Office, 2008, p. 33-41).

As well, the DHS established in 2003 the National Cybersecurity Division which then further led to a creation of US-CERT to coordinate cyber security efforts, and analyze, identify and reduce possibility of cyber-attacks (Fischer, 2005, p. 50). In December 2004, the DHS released one of the first reports called Cybersecurity for the Homeland. The paper stresses the significance of the security of cyberspace, and the protection of critical infrastructure. Furthermore, it demonstrates the focus of this federal department on cyber security, its cyber-related divisions, and the future plans for the expansion in this area (Chairman and Ranking Member Subcommittee on Cybersecurity, Science, and Research & Development of the U. S. House of Representatives Select Committee on Homeland Security, 2004, p. 3-6). The importance of this federal department was then presented in the CRS Report for Congress which confirmed its position within the cyberspace framework of the U.S. (Fischer, 2005). Since 2006, the DHS started testing the national preparedness against cyber-attacks (including the private and public sector) by conducting the so-called cyber storms (DHS, 2018a).

On March 26, 2007, President George W. Bush signed the Homeland Security Presidential Directive – 16: National Strategy for Aviation Security which did not specifically concentrate on the DHS, but it yet again, put the emphasis on the protection of the critical infrastructure in the realm of cyberspace which has been previously appointed to the DHS (U.S. Government Publishing Office, p. 2008, p. 96).

Then, in January, 2008, President George W. Bush established the Comprehensive National Cybersecurity Initiative (CNCI) in National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23). One of the main reasons for its establishment was an enhancement of cyber security resilience of the U.S. with the help of federal agencies including the DHS. Its task includes expansion of education about cyberspace, development of counterattack strategies, strengthening of counterintelligence capabilities, increasing government investment into cyber security, or information-sharing between federal agencies, and public and private sector (Rollins, Henning, 2009, p. 5-7). The DHS has been chosen as a department to deal with the private-public sector information sharing (ibid, p. 7).

4.2.2. Process tracing of 9/11 events

Process tracing encompasses four tests that either confirm or reject the hypothesis with the use of evidence that holds different probative value (Bennett, 2010, p. 2-4). However, it is possible to decide which test is the most suitable for a certain situation by outlining the sequence of events

(Collier, 2011, p. 829). Thus, after this step is done in this chapter, the smoking-gun test is chosen to be taken. Passing the test itself provides a sufficient but not necessary criterion for accepting the hypothesis while failing to pass does not fully reject it (Collier, 2011, p. 826). The hypothesis (H1) set out in this thesis is that the securitization of cyberspace and cyber security took place after the events of 9/11 which served as a strong catalyst that put this idea into practice. As a competing hypothesis (H2) by Myriam Dunn Cavelty (2008) who argues that the cyber threat debate is a case of the failed securitization because there have been no exceptional measures (policies, or a strategy) trying to resolve the governance of cyberspace.

To start, hypothesis 1 is examined. Before 9/11 there have been documents relating to cyberspace such as NSDD-145, and the PCCIP was established. Additionally, new terminology was created that framed cyberspace as an area with a hidden threat that could be exploited by terrorists and bringing devastating effects to the whole country. The findings of the PCCIP stressed the need for an increased attention to this area while it has also been mentioned several times in the documents and reports that cyberspace is often used by terrorists and criminals. Yet, there were no calls for extraordinary measures (Bendrath et al., 2007, p. 67), and there was almost no institutionalization, major policy initiative, or a national strategy regarding the cyber related issues. On the other hand, right after 9/11, even though the focus was on terrorism, the Bush administration released the National Strategy to Secure Cyberspace in 2003, followed by HSPV-7. Moreover, the DHS was tasked with the information security from the very beginning of its existence, which was further supported by the creation of National Cybersecurity Division or as it is called today US-CERT in 2003. This demonstrates that actual action, policy changes, institutionalization or national strategies were pursued after the events of 9/11, thus, presenting the calls for extraordinary measures which could be seen in these documents. Therefore, there is a difference in an approach to cyber security and cyberspace before the events, and after it. Despite the fact that the warnings against the cyber-related threats have been there before, 9/11 served as the main catalyst that allowed for the securitization of this area. The presented clues support the hypothesis that the securitization of cyberspace and cyber security took place after the events of 9/11 which served as a strong impetus that put this idea into practice.

The second hypothesis states otherwise. As it was previously mentioned, before the events, there was a widely spread rhetoric about the dangers of cyberspace but there were no significant actions to support it. Directly after 9/11, the main change could be traced back to the DHS and its

new task regarding the protection of critical infrastructure in cyberspace, and information security. Many things remained similar such as the discourse about the dangers of cyberspace, or areas marked as critical (Cavelty, 2008, p. 27). However, without any doubt, the call for the extraordinary measures became a reality. There was an institutionalization of cyberspace within the DHS in the area of information security, and protection of critical infrastructure in cyberspace. The National Strategy to Secure Cyberspace in 2003, HSPV-7, or the establishment of US-CERT interfere with the notion that there were no significant changes after 9/11 within the cybersecurity area, and thus confirm the first hypothesis. With a weaker interpretation of the policies, strategy, and institutionalization of cyberspace, it still makes H1 more plausible than H2. The smoking-gun test concludes that there has been a securitization of cyberspace after the 9/11 which served as an important catalyst that set things into motion because it offered an opportunity to proceed with it. Furthermore, even with the weaker interpretation, H1 appears to be more likely than H2 which again confirms the hypothesis set out in this thesis.

In a wider historical causal chain, the 9/11 catalyst moment can be pinpointed back to the Reagan era where there were first publicly voiced concerns about the cyber security and the possible breaches to obtain classified information. The following administrations stuck with the initial rhetoric, and modified it with the technological advancements. The progress also brought to light new challenges which could have been then used to point out new arising dangers of cyberspace. However, there was not a real opportunity to securitize cyberspace. This window opened with the 9/11 events which rounded off the long term ongoing threat framing rhetoric from 1980s.

4.2.3. The Obama Administration

Significant changes came with the new President Barack Obama who took office on January 20, 2009. However, he continued with the similar rhetoric as his predecessor George W. Bush. One of the first documents of the new administration relating to cyberspace was Cyberspace Policy Review from May, 2009. The report was released by the National Security Council and the Homeland Security Council, thus, the DHS directly cooperated on it. The review laid out a plan for improvements within the cyber security area, it identified potential threats of cyberspace, and yet again demonstrated the importance of the dialogue between the private-public sector. Moreover, it emphasized the role of the federal government as the one to tackle the problems

relating to cyberspace, and the cooperation between the sectors, as well as the need to keep up with the threat (DHS, 2009, p. 5-9).

Although, not directly related to the DHS, the event from June, 2010, affected the cyber security, and also in a way perception of cyberspace as a whole. On that day, the Stuxnet worm was implanted into the computer systems in the Natanz nuclear facility in Iran. After that it specifically targeted the networks controlling the uranium centrifuges, while also recording the normal operation process, and replaying it to the staff of the facility to deceive them into thinking that everything was in order. It further changed the frequencies of the centrifuges resulting in the destruction of 1,000 out of 9,000 of all of them (Steed, 2015, p. 81-83). Supposedly, there were two governments behind it – Israel, and the U.S. – but it has never been fully confirmed. However, this event was the first account of an actual physical damage done with the use of cyber related means. In a way, it could be seen as a materialized fear that cyberspace could one day cause an actual physical damage. It may have amplified the ongoing securitization of the area which began with the events of 9/11.

On March 30, 2011, the Presidential Policy Directive-8 (PPD-8) was released which designated the DHS to create the National Preparedness system to enhance the security and resilience of the U.S. This was supposed to be achieved by systematically preparing the U.S. against various threats encompassing even cyber-attacks while the protection capabilities specifically included area of cybersecurity (Obama, 2011). In May, 2011, another cybersecurity document came into existence – International Strategy for Cyberspace where the U.S. sought to promote norms, and the protection against cyber related threats in the national and international environment (The White House President Barack Obama, 2011).

However, in October, 2012, President Barack Obama signed one of the most controversial directives – Presidential Policy Directive 20 (PPD-20) which complemented the NSPD-54/Homeland Security Presidential Directive HSPD-23, and at the same time superseding National Security Presidential Directive-38 (Obama, in Federation of American Scientists, 2012, p. 1). These documents allowed the surveillance of foreigners suspected of terrorism, and further led to a surveillance of American citizens as well (Kapto, 2013, p. 360). The directive was signed in secret, and became public on June 7, 2013, after Edward Snowden released it to public through the Guardian (Greenwald, MacASkill, 2013). It was directed at the establishment of processes, principles, protection, and uses regarding cyberspace and cyber security. Furthermore, it

specifically enables the government of the U.S. to conduct Defensive Cyber Effects Operations (DCEO) and Offensive Cyber Effects Operations (OCEO) (Federation of American Scientists, 2012, p. 4). It admits the fact that these operations may have unintended consequences or even collateral damage because of the interconnected nature of cyberspace (ibid, p. 6). In specifically defined situations such as self-defense, or the country's interests, the U.S. would not have to obtain consent from a country where cyber effects would be expected to occur (ibid, p. 7). Moreover, it distinguishes between cyber defense, and cyber offense (or operations) (ibid, p. 8-9). The mention of the cyber offense is significant because up until this point all the previous documents focused on the defense against the attacks aimed at the U.S., and protection against these threats. In this case, the use of cyber capabilities against other actors was admitted which made it part of the offensive tools which could be deployed by the U.S. government. Additionally, the DHS was assigned as the main agency to protect the critical infrastructure, and the relation with private sector (ibid, p. 8). Under particular circumstances, the Secretary of Defense, or an authorized person may conduct Emergency Cyber Action which would mitigate an imminent threat in cases where there would be no time to obtain Presidential approval (ibid, p. 10). The National Security Staff was tasked to formalize the functions of the Cyber Operations Policy Working Group (COP-WG) which became the main cyber policy forum (ibid, p. 11). The last development triggered the processes to establish the framework for the protection of the U.S., as well as stating the goals already set in previous documents such as interagency cooperation, leading efforts to establish international consensus etc. (ibid, p. 14-18).

Despite the fact that the directive called for the protection of U.S. persons, it still did not prevent the surveillance conducted by the U.S. federal agencies (NSA) through the program called Prism (BBC News, 2014; Federation of American Scientists, 2012, p. 13). Cyber surveillance plays a significant role within the broader surveillance practices. With the technological progress, more information and data started appearing online, in data storages, clouds or computer themselves. This on one hand increased the accessibility of these data, on the other hand also made them more prone to attacks. In the terms of surveillance, while it helps uncover, investigate and prevent criminal activity, it can also be accessed through malicious software by criminals or terrorist groups. At the same time, the cyber surveillance may be illegal, and even conducted by the citizens' government without their knowledge like in the case of the program Prism. Moreover,

almost all web traffic is monitored where one of the examples can be the third party monitoring[1]. The information harvested by the corporations could then be sold to third parties for their own profit such as influencing people's opinion, or political purposes. This happened in 2018, when the Facebook-Cambridge Analytica scandal came to light where Facebook shared data of up to 87 million user profiles with political consulting group Cambridge Analytica (Kang, Sheer, 2018). This points to a disturbing reality where one's privacy might be threatened, and the information used against oneself.

Then on February 12, 2013, President Obama signed another Executive Order – Improving Critical Infrastructure Cybersecurity. It aimed to build improvements for the protection and resilience of the critical infrastructure through the enhancement of information sharing, development of a framework reducing the cyber risks, or identification of major weakness where 'the catastrophic effects' may occur. The DHS was tasked with assessing the privacy and civil liberties risks, adoption of the newly created framework, and the preparation of a report talking about cyber-related risks (Obama, 2013). On the same date, President Obama also signed Presidential Policy Directive - Critical Infrastructure Security and Resilience which further expanded the role of the DHS within the area of protection of critical infrastructure. It required the department to coordinate with the public and private sector, coordinate responses to physical and cyber incidents, report annually on the status of the critical infrastructure. The cooperation is significant because most of the critical infrastructure is owned and operated by the private sector which makes it the first line of defense against possible cyber threats. Thus, the information and data sharing, and communication between these two sectors is crucial for the resilience of the nation. Likewise, private sector provides cyber security for businesses, corporation, and other actors which again required cooperation with the public sector to enhance the overall protection. Moreover, the DHS was supposed to create two national infrastructure centers – one for the physical infrastructure, another one for the cyber infrastructure – while admitting their inherent link. Additionally, the Information Technology sector was assigned to the DHS alone (The White House, 2013). This of course enhanced the position of the DHS within the cyber security, and

[1] It is a "the practice by which an entity (the tracker), other than the website directly visited by the user (the site), tracks or assists in tracking the user's visit to the site." For more information, see Roesner, F., Kohno, T. and Wetherall, D., 2012, April. Detecting and defending against third-party tracking on the web. In Proceedings of the 9th USENIX conference on Networked Systems Design and Implementation (pp. 12-12). USENIX Association.

consolidated its institutional role in this area. Likewise, it could have led to the increased agenda-setting power.

As of January 13, 2015, President Obama announced a new cybersecurity legislative proposal that was emphasizing the need of an enhanced protection against the 'unprecedented threat' of hackers, and other actors such as criminal organizations or even state actors. In addition, it called for better information sharing between the public and private sector which was yet again assigned to the DHS, enhancement of law enforcement in the area of cybersecurity, or reporting on national data breaches (The White House, 2015).

The Presidential Policy Directive 41 – Cyber Incident Coordination Policy from July 26, 2016, institutionalizes approaches, and particular steps of the Federal government in case of a cyber-incident, as well as the coordination of federal agencies, their role division, and the subsequent restoration process. The role of the DHS in case of a major cyber related incident, is to be the lead federal department to coordinate response activities, while also gathering information about the incident to make a report which would help others prevent similar situation. In cooperation with the Department of Justice, the DHS is tasked with informing the public and private sector (The White House, 2016).

The 2016 presidential elections were hit with one of the biggest cyber hacking incidents in modern history. Russia has been accused of interfering in the elections by eight U.S. Intelligence Agencies (Yourish, Griggs, 2018). Allegedly, they were supposed to use state-backed media, fake social media accounts to post false stories, and lead the so-called 'information warfare' against the U.S. to disadvantage presidential candidate Hillary Clinton (Masters, 2018). While there are many different definitions of what information warfare is, one of the most encompassing definitions by the DoD defines it as '…actions taken to affect adversary information and information systems while defending one's own information and information systems. IO apply across all phases of an operation, throughout the range of military operations, and at every level of war. Information warfare (IW) is IO conducted during time of crisis or conflict (including war) to achieve or promote specific objectives over a specific adversary or adversaries.' (Joint Chief of Staff, 1998). In response to these attacks, the Special Counsel Investigation (Mueller Investigation) was created which is a law enforcement investigation looking into Russian efforts to meddle with the elections. Up until now, at least 34 people and three companies have been charged (Rodriguez, Jin, 2019).

However, even with the overwhelming evidence, President Donald Trump keeps refusing to admit the nature of these events (Yourish, Griggs, 2018).

4.2.4. The Trump Administration

Yet again, changes came with a new administration when President Donald Trump took the office on January 20, 2017. Firstly, the U.S. Government Accountability Office (GAO) filed a report to Congressional Committees on Cybersecurity which came to the conclusion that DHS's National Integration Center generally performed required functions but it needed to evaluate its activities more completely (GAO, 2017, p. 2). However, a year later, on April 24, 2018, for the testimony before the Committee on Homeland Security and Governmental Affairs, U.S., the report stated that the efforts of the DHS in the area of promotion and improvement of federal and private-networks needed to be strengthened. Although, it made certain progress, and released a Framework for Improving Critical Infrastructure Cybersecurity, it was enough to mitigate the threats encompassed within cyberspace. Additionally, the DHS itself did not reach the number or required workforce in the field that would possess the critical skills. One of the main issues also presented the insufficiency of reporting on cyber risk mitigation in eight critical infrastructure sectors (GAO, 2018, p. 2).

The first document related to cyberspace signed by President Donald Trump was issued on May 11, 2017, called the Executive Order on Strengthening the Cybersecurity Federal Networks and Critical Infrastructure. It aimed at an improvement of the U.S. capabilities in the area of cyberspace by modernizing the federal IT infrastructure, enhancing the relations and cooperation between the public and private sector, as well as cooperation with countries allies. It stressed the inadequate attention the field has been given, the need for implementation of risk management measures. Every agency and department was required to use the Framework for Improving Critical Infrastructure. Furthermore, it emphasized the position of the DHS within the cyber security field, and in a way promoted the DHS as the main department to tackle cyberspace issues. It specifically targeted areas such as botnets, response to electricity disruptions, and further called for immediate improvements of cyber security, and most importantly the relation between the public and private sector (Trump, 2017).

President Donald Trump is more invested in cyberspace and cyber security more than his predecessors. Since the responsibilities of the DHS expanded, on May 15, 2018 it released a document called U.S. Department of Homeland Security Cybersecurity Strategy. Furthermore,

after the 2016 election interference, it became evident that the level of protection in the area of cyber security is not sufficient. This was further demonstrated during the ransomware attacks in 2017 including WannaCry, Petya and NotPetya which together hit thousands of computers worldwide, including facilities such as hospitals or government buildings (Symantec, 2017; Hern, 2017).[2] Additionally, the DHS has kept reports of all attempts to breach government networks between 2006 and 2015 which uncovered inadequate resilience of the systems. This paper set out the framework for the execution of cyber related responsibilities of the DHS for the next five years (DHS, 2018b, p. 1). The goals of the department range from identification of cyber security risks, through reduction of the threats, to better cyber security management within the department (ibid, p. 3).

One of the major moments in the U.S. regarding the cyber security was the release of the National Cyber Strategy of the United States of America signed by President Donald Trump on September 20, 2018. It is one of the first national cyber security strategies in nine years. The main goals consist of protection of networks, systems, and data, provision of security to digital economy, or an improvement of resilience against cyber threats (The White House, 2018, p. 1). It points at the threatened state of the U.S., and the growing capabilities of its competitors. Moreover, it specifically mentions states such as Russia, Iran, North Korea or China, and their cyber-related incidents against the country (ibid, p. 1-2). Overall, it focuses on the protection against cyber threats, enhancing the role and effectiveness of federal agencies tasked with cyber related tasks, strengthening the resilience, supporting the American economy, or increasing the position of the U.S. in the international cyber security arena (ibid, p. 3-5). Additionally, the DHS was yet again appointed one of the lead departments to tackle cyber security, and secured Federal department and agency networks (except DoD and Intelligence community) which gave it exclusive access to their networks (ibid, p. 6-7). It was supposed to further continue the oversight of the public and private sector (ibid, p. 7).

On November 15, 2018, President Donald Trump signed a measure called the Cybersecurity and Infrastructure Security Agency Act of 2018 which reorganized and renamed the initial cyber security division within the DHS National Protection and Programs Directorate into

[2]Ransomware could be defined as a malicious software that uses computer system's vulnerability to encrypt its files, and demands to be paid a ransom to unlock the files. For more information, see Luo, X. and Liao, Q., 2007. Awareness education as the key to ransomware prevention. Information Systems Security, 16(4), pp.195-202. Available online: https://www.tandfonline.com/doi/full/10.1080/10658980701576412

Cybersecurity and Infrastructure Security Agency (CISA). One of the main changes was the transfer of the Office of Biometrics Identity Management (OBIM) to the DHS's Management Directorate, and it gave a power to the Secretary of Homeland Security to decide on the organization of the Federal Protective Services. Furthermore, this agency works independently on the DHS. Its main efforts encompass protection of critical infrastructure, cyber defense to the Federal government but also public and private sector, or communication and response system to cyber incidents (DHS, 2019).

After the events of 9/11, and the creation of the DHS, cyberspace and cyber security were framed in terms of possible threats, tools of terrorist, and the critical infrastructure vulnerabilities. While different administrations realized the benefits of these areas, they mostly concentrated on the risks stemming from them. The Bush administration mainly covered the area of the protection of critical infrastructure, whilst the DHS started setting up different divisions of cyber security, as well as more competencies began being transferred to this federal department. This trend continued even during the Obama administration which deepened commitment of the government to tackle cyber related threats, critical infrastructure protection, as well as the need for better communication between public and private sector. However, major difference can be found in the expansion of cyber operations – DCEO and OCEO – which also differentiated between cyber defense and offense. It further enlarged the capabilities of the DHS in the cyber security area, assigned it a special position in case of a major cyber incident, and created a cyber-infrastructure center. Moreover, this administration was more active in releasing documents, strategies, and policies compared to the Bush administration. It also deepened the focus on the economic benefits, and digital economy, and interconnectedness provided by cyberspace.

Lastly, the Trump administration also widely concentrates on cyber security and cyberspace so far, releasing the cyber security strategy, and creating a separate body from the DHS to deal with cyber related issues. Additionally, the DHS was appointed to be the leading federal department in cyber security of the U.S. The election hacking incident was reflected in the documents by for example adding passages about botnets, or specifically naming the ‘adversaries’ of the U.S. In general, similarities in the approaches can be seen across the different administrations including critical infrastructure protection, the need for information sharing, cooperation between public and private sector, the inadequate contemporary measures, international cooperation or the stress on the possible devastating effects of cyber-attacks. This

could be explained by the securitization that took place after 9/11, and framed cyberspace and cyber security as an area of vulnerabilities and threats. As the new cyber incidents started appearing, the discourse evolved with them, which could be seen for example after 2010 Stuxnet after which PPD-8 was released that aimed at increasing cyber resilience. Likewise, the growing number of benefits of this field reflected in documents, policies and strategies of each administration, as well as the attempt to claim primacy in this area. Since the establishment of the DHS, it gradually received wide range of responsibilities and capabilities which expanded with every new administration. This further signifies the leading position of this federal department in cyber security area of the U.S., and gives it more power in pushing its own agenda onto the national strategy. It could also mean that each of the administrations trusted or trusts the DHS to tackle this kind of protection, and leaves decisions up to it which yet again increases its agenda-setting power in this respective area.

The historical analysis has shown that there has been a securitizing discourse in regards to cyberspace before the 9/11, however, the event served as a catalyst that led to the securitization of the field. Moreover, it also legitimized the urgent need for the establishment of a homeland security institution which is the DHS. Furthermore, cyberspace and cyber security have been framed as a potential threat to the nation, and the protection against risks stemming from them became a priority. In the upcoming years, different administrations generally continued with the deepening the cyber resilience, yet, each expanded into new areas but the focused remained the same. Additionally, the DHS has been tasked with the cyber security from its very beginning, and its powers gradually expanded over time to the point where it became the leading federal agency in the field. It could have ultimately given it more power to push its agenda in this area onto other actors, and the documents related to it. Moreover, expansion of powers with every administration may signal that the trust with the department has increased over time which solidified its agenda-setting powers in cyber security. The following chapter illustrates the role of the DHS within this respective area, and provides a comparison with other federal agencies and departments in this field to demonstrate its specific position among them.

5. The role of the DHS in cyber security

The following chapter presents the internal structure of the DHS tasked with cyber security and cyberspace protection. It is necessary to show the divisions of the DHS in order to fully imagine the scope of its responsibilities and capabilities in relation to cyber security. Furthermore, it uncovers the reach of the department which may strengthen its agenda-setting powers in this respective area, and facilitate pushing its policies and ideas onto the national cyber security strategy. It also demonstrates a certain link between critical infrastructure and cyber security which has been mainly established during the Bush administration.

5.1. Cyber security and the DHS

Over the years, the DHS released many guidelines, documents and initiatives referring to cyberspace. It also provides cyber security frameworks for specific sectors including for example the chemical sector, transportation systems, dams or the federal framework (United States Computer Emergency Readiness Team, n.d.). Initially, the DHS consisted of many cyber security divisions fulfilling different tasks. However, in November, 2018, President Donald Trump signed an act called Cybersecurity and Infrastructure Security Agency Act of 2018 which reorganized and renamed the initial cyber security division within the DHS National Protection and Programs Directorate (NISA) into Cybersecurity and Infrastructure Security Agency (CISA). This was a significant change since it may have given the DHS under its influence a powerful agency combining cyber security and critical infrastructure while also expanding the actorness of the federal department. By elevating this security federal entity, it indicated the importance of the areas involved, and potentially highlighted the need for their better protection. In general, it concentrates on the cyber security and resilience of the nation against cyber related threats. It further mediates the relation between the public and private sector, it develops emergency communications capabilities, and provides support for other actors (DHS, n.d.a).

CISA encompasses a wide array of divisions. First, the main task of the cybersecurity division is to protect the federal gov. domain, and cooperate with civilian government com. in order to increase their resilience. It is done through four subdivisions. To start, it is the National Cybersecurity and Communications Integration Center (NCCIC) which aims at the reduction of cyber and communications risks, while also providing cyber and communications information, technical expertise, and operational integration (DHS, n.d.b). Next, there is the Stakeholder

Engagement and Cyber Infrastructure Resilience (SECIR) which mediates and sustains the partnership between various actors from private and public sector to reach longer cyber risk management (DHS, n.d.c). Federal Network Resilience (FNR) specifically ensures cyber security support and coordination to all federal executive branch agencies such as models, designs and training in this respective area (DHS, n.d.d). Lastly, the Network Security Deployment (NSD) is a division that works on the improvement, development, and integration of various cybersecurity products, services, and technologies. It further incorporates the National Cybersecurity Protection System (NCPS) working on the so-called EINSTEIN set of capabilities, the Continuous Diagnostics and Mitigation (CDM) mainly allocating cybersecurity resources, and the Enhanced Cybersecurity Services (ECS) focusing on the intrusion prevention capability (DHS, n.d.e; DHS, n.d.f; DHS, n.d.g). Another separate division is the Emergency Communications Division which supports and promotes communications that are used by emergency responders and government officials, as well as communication preparedness in case of an emergency. It provides various trainings and tools to different actors from both public and private sector (DHS, n.d.h). Another major division is the Infrastructure Security Division. It is a cross-sector division assessing the vulnerabilities and possible consequences of risks to critical infrastructure.

Moreover, it estimates new risks and hazards, and provides tools and advice on how to deal with them (DHS, n.d.i). It has six subdivisions. First, the Infrastructure Information Collection Division (IICD) aims at providing technology solutions to nation's critical infrastructure data which are then passed to federal, state, and local governments so they can make better decisions, and better prepare for possible disasters. It further includes two main program – the Infrastructure Protection (IP) Gateway for secure collection, and sharing of data; and the Protected Critical Infrastructure Information (PCII) Program which specializes at protection of sensitive data shared with the DHS (DHS, n.d.j). Subsequently, the Infrastructure Security Compliance Division (ISCD) is tasked with the implementation of the Chemical Facility Anti-Terrorism Standards (CFATS), and at this point proposed the Ammonium Nitrate Security Program (DHS, n.d.k). Then, the National Infrastructure Coordinating Center (NICC) manages coordination and information sharing center for federal government which functions as an intermediary between the DHS and the third-party facility in case of an incident (DHS, n.d.l). Fourth, the Protective Security Coordination Division (PSCD) is responsible for providing necessary programs, guidance, and initiatives that strengthen the security and resilience of the national critical infrastructure (DHS,

n.d.m). Next, the Sector Outreach and Programs Division (SOPD) provides tools, resources to different sectors, while also serving as a sector specific agency for six critical infrastructure sectors (DHS, n.d.n). Lastly, there are 16 Critical Infrastructure Sectors in total which are in a way considered to be divisions of their own, and are subsequently responsible for their protection (DHS, n.d.o). The last division is the Federal Protective Service whose mission is to respond and help with the recovery from various disasters, and building of security (DHS, n.d.p).

Part of the CISA is also the National Risk Management (NRMC) which pursues the identification of the biggest risks to the national critical infrastructure. In order to do that, it is divided into six subdivisions which cover the most important areas. Initially, the Cross Sector Risk Management focuses on the risk analysis, planning, and interagency partnership to enhance the resilience and protection in this respective area (DHS, n.d.q). Following, the Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force develops new strategies to enhance the ICT supply chain, and protect it against cyber related threats. It partners up with many companies across the industry to ensure their protection (DHS, n.d.s). After that, the National Critical Functions Initiative works to protect the critical functions of the public and private sector throughout all 16 critical infrastructure sectors. Furthermore, it assesses perform risk analysis, dependency analysis, and consequences modeling to highlight main vulnerabilities (DHS, n.d.t). Next is the Pipeline Cybersecurity Initiative which focuses on identification and mitigation of risks to pipelines across the U.S. (DHS, n.d.u). Then, the Tri-Sector Executive Working Group facilitates the partnership between the public and private sector integrating the risk management into financial, communication, and electricity sectors (DHS, n.d.v). Ultimately, the CISA also provides the Election Security which secures the physical and cyber infrastructure against external intervention, and ensures resilient and secure election process (DHS, n.d.w).

The chapter demonstrated the complex structure of the cyber security division CISA of the DHS whose tasks have been expanded over the years since its foundation. It reaches to various sectors, industries and even other federal agencies. Additionally, the division consists of two main parts – cyber security and critical infrastructure. This presents an interesting reality which can be traced back to the Bush administration where the main concerns about the dangers of cyber threats were to the critical infrastructure. It then again points at framing of cyberspace as a danger to the vital part of the nation. Moreover, the outreach of the agency raises its trustworthiness in this

respective area. It can make its decisions pursuing strategies, setting frameworks, or just assisting the government with cyber related documents more credible, and thus, less likely to be questioned. Likewise, its seemingly rich expertise can allow it to easier push its own agenda onto other actors, and even a national strategy. Since it manages and administers most of the cyber tasks, it then may seem rational to be require advise from this agency, and implement its recommendations, and policies into other governmental documents.

5.2. Other federal agencies, actors and cyber security

The DHS is of course not the only federal department and agency tasked with the cyber security, although, it has been appointed as the leading department in this area, especially after the internal reorganization and foundation of the CISA. This following chapter briefly summarizes the focus and missions of other federal departments and agencies in the area of cyber security and cyberspace. It is necessary to demonstrate the specific position of the DHS compared to the other federal departments and agencies in order to reveal its agenda-setting powers in cyber security, as well as cyberspace. Moreover, it also shows the complex network among federal agencies and departments in the field of cyber security and cyberspace which explains their importance, and thus, the significance of the topic of this thesis as well.

5.2.1. National Security Agency (NSA)

NSA holds a specific position when it comes to cyberspace and cyber security in the U.S. It was founded on November 4, 1952, when the Secretary of Defense decided to act under specific instructions from the President in the National Security Council. The agency acquired responsibility for the Communications Intelligence (Comint), a year later for Communication Security (Comsec), and in 1958 also for Electronics Intelligence (Elint) (Howe, 1974, p. 11). Its main goals were defined in the National Security Council Intelligence Directive No. 9 (NSCID-9), which tasked it with the effective management of communication intelligence activities of the U.S. against foreign governments (Truman, 1950). Thus, the NSA has been involved in the area of technology since its establishment. While the focus of the agency changed, especially since 9/11, the agency acquired more responsibilities in the area of technologies and communications, more specifically in cyber security. Currently, its mission encompasses a protection of National Security Systems (systems including classified information), monitoring adversaries developing cyber capabilities, innovation of technologies, as well as running 24/7 cyber operations to protect

the nation. Other activities include promotion of cyber security knowledge and guidance, or a support of cyber security professionals (NSA, n.d.a). The NSA is further responsible for Signal Intelligence (Sigint), and passing the vital information to nation's policy makers and the military. It gathers information on foreign powers, organizations, terrorists or people for all the departments of the Executive Branch of the U.S. government (NSA, n.d.b).

5.2.2. Federal Bureau of Investigation (FBI)

While the FBI has a long history as the main law enforcement agency in the country, it also received tasks regarding cyber security and cyberspace. More specifically, in July, 2002, the FBI established its Cyber Division which prioritized Cyber Crime. Among other tasks, its mission included: 1) cyber related federal violations by terrorist groups, foreign governments intelligence operations, or criminal activity related to that; 2) supporting public and private partnership, and provision of education and guidance; and 3) boosting the position of the FBI's cyber investigation capabilities by following new technologies and awareness (Monroe, 2003). Additionally, in the National Strategy to Secure Cyberspace from 2003, the agency was under the DoJ assigned to 'lead the national effort to investigate and prosecute cybercrime.' (FBI, n.d.a). Currently, the agency sees its priorities in investigating cyber-attacks by criminals, adversaries, and terrorists because it combines protection of the national security while also being the main law enforcement agency (ibid). Especially in the area of cybercrime, the FBI focuses on the computer and network intrusions and ransomware, while other related tasks include identity theft, or investigation of online predators (FBI, n.d.b). Furthermore, the agency also manages the Internet Crime Complaint Center (reporting mechanism for citizens for suspected webpages), Cyber Action Team (the deployment group of cyber experts which investigates cyber intrusions), and National Cyber Forensics & Training Alliance (alliance for sharing knowledge, information, and resources across the public and private sector) (ibid). Moreover, in 2008, the National Cyber Investigative Joint Task Force (NCIJTF) was established, serving as a multi-agency cyber center aimed at coordination and sharing information in order to better address investigation of cybercrimes (FBI, n.d.c). Likewise, the FBI also sees part of its mission to support the DHS through the investigation of cyber related crimes which ultimately increase the protection of the national security (FBI, n.d.a).

5.2.3. The Department of Defense (DoD)

Not exactly a federal agency, yet, the DoD is a major actor in the cyber security area in the U.S. Just like the NSA, the DoD has a long history and experience with the technological area. Already in 1972, DoD warned against the vulnerabilities and risks tied to the network and information security. However, the first cyber division was established in 1998 called Joint Task Force-Computer Network Defense (JTF-CND). It focused on the protection of military services and DoD networks. One of the most important changes came on November 12, 2008, the Secretary of Defense Robert Gates established the U.S. Cyber Command (USCYBERCOM). After 2002, these responsibilities fell under the U.S. Strategic Command (USSTRATCOM). Then, on June 23, 2009, it also merged the Joint Task Force - Global Network Operations (JTF-GNO) and Joint Functional Component Command for Network Warfare (JFCC-NW). It also created the 'dual-hat' between NSA and USCYBERCOM which formed a special relation between them. Furthermore, on August 18, 2017, the USCYBERCOM became a Unified Combatant Command tasked with cyberspace operations, followed by 2018 when it transformed into CCMD (U.S. Cyber Command, n.d.a). The division is mainly responsible for the protection of the DoDIN, support for combatant commanders, and increasing the cyber resilience of the nation (U.S. Cyber Command, n.d.b). Moreover, it concentrates on the coordination of cyberspace planning and operations in order to protect the U.S., and pursue national interests in cooperation between domestic and international partners (ibid). Just like the DHS, the DoD released its own Cyber Strategy in 2018 in which it identifies its main objectives as 1) assurance that Joint Force is able to achieve its missions; 2) the Joint Force would conduct operations in cyberspace to ensure military advantages of the U.S.; 3) protection of the U.S. critical infrastructure against cyber threats; 4) securing the DoD information and data; and 5) mitigating cooperation with other actors (DoD, 2018, p. 3). Likewise, the department aims at enhancing the cyber capabilities of the U.S. military to be able to better deter threat, and fight wars (ibid, p. 2).

5.3. Does the DHS hold a special position in cyber security?

As this chapter demonstrated, other federal agencies or an executive branch department are vested in the area of cyber security and cyberspace. Together with the DHS, they created a complex network of protection against cyber threats, or even possess some offensive tools. Moreover, the DHS has a wide range of responsibilities and capabilities in cyber security compared to these other

actors. The NSA has been involved in the area of technologies since its foundation, however, in cyber security it is rather limited to protection of National Security Systems, monitoring and gathering information, and in a way innovation. Then, the FBI is responsible for tackling mainly cybercrime, investigation of cyber incidents but also for the support of the DHS, and cooperation with this agency. Lastly, the DoD focuses on the military related cyber security and capabilities. However, compared to the other actors, it shares more similar objectives with the DHS than the other two. In general, the missions and goals of these actors do not overlap, and create a network of protection for the U.S., although, its adequacy is questionable. Likewise, the mutual objective for these actors is the protection of the nation, and in most cases the protection of the critical infrastructure of the U.S. This could have several explanations. First, in case of a cyber-attack, critical infrastructure would be the ideal target, since the impact of a successful attack might be tragic. Therefore, significant amount of cyber security efforts would go to the protection of these sectors since they are vital for the continuous functioning of the country.

Another explanation could be that the government has mostly responsibility for the protection of the critical infrastructure, and therefore, it tries to largely invest into its protection. Out of the three outlined explanations, this one is the least likely reason since around 85% of the critical infrastructure is owned and run by the private sector (U.S. Chamber of Commerce, n.d.). Lastly, tying cyber security to the critical infrastructure protection could allow the government to facilitate proposed legislations changes because these sectors are crucial for the proper functioning of the country. Thus, it might then be easier to pass certain changes within the cyber security area, and continue with the threat framing rhetoric rather than just stating the more 'regular' challenges. Moreover, it is in contrast with other actors in the field such as the EU which emphasizes rather a normative approach involving soft power, protection of fundamental rights, resilience, or education (Christou, 2017). The combination of the first, and the third explanation seem to be the most likely explanations for this connection. Taken into account the historical events after the 9/11, vast number of the documents included, or were specifically aimed at the protection of the critical infrastructure in the cyber realm. While on one hand, it is necessary to fortify its resilience, on the other hand, it could have also been used to ease up the process of passing measures tied to cyber security.

After outlining the different tasks, the federal agencies and departments have in cyber security, it also provides a better understanding of the U.S. cyber security strategy. The objectives

and assigned areas of protection show their extensive reach, however, there are a few that stand out and could be latter found on the national level. The main concern seems to lie within the protection of the nation, critical infrastructure, national security but also the military. This also helps explain the specific approach the U.S. has towards this respective field, as previously mentioned, compared to the EU. Furthermore, it shows the complexities and the significance the national cyber security strategy possesses because it determines the changes within this scheme which can ultimately give more power to one actor over the rest, or disrupt the proper functioning of this system. The impact could be far-reaching, and thus, it is necessary to present the stand of the U.S. towards cyberspace.

Another interesting factor has demonstrated throughout past two chapters. Based on the evidence, including the historical events, there may be a special relation between the presidency and the DHS. These two actors have been in a close cooperation since the federal department was established on the impulse of the president in 2002. Over the years, the power in cyber security has been gradually redirected to the department by this respective actor who has also ordered to create CISA, one of the most importance bodies dealing with cyberspace in the U.S. Other federal offices may have not received the same treatment which can be seen in their assigned tasks. Additionally, certain types of leadership and focus of the president led to an expansion of responsibilities of the DHS in certain areas. For illustration, the Bush administration mainly focused on the protection of critical infrastructure in the light of the at the time recent 9/11 terrorist attack. The administration was active in both, domestic and foreign policy, however, the powers within the DHS mainly concentrated on the domestic protection. Then, the Obama administration, continued with the changes which started with the previous government, however, it increasingly stressed the need for cooperation with the allies of the U.S., e.g. International Strategy for Cyberspace from 2011. In addition, it has admitted the use of offensive cyber measures, and assigned the DHS a special role in case of a major cyber incidents. Most of the changes were suggested through policy directives, legislative proposals, or policy reviews. Finally, the Trump administration is majorly invested in cyberspace the changes so far have been implied by executive orders, or the president and the NSC themselves. Also, they have mostly targeted domestic policies and amendments, rather than the foreign aspect. It is also visible, that the context of each administration affects the areas that get ultimately adjusted.

Nevertheless, federal agencies and departments are the front of defense against threats stemming from cyberspace, and in the era of fast technological advancements it is necessary to address their position within this area. Furthermore, this chapter showed that the DHS has more responsibilities and capabilities in cyber security than the other presented actors which increases its agenda-setting power, and could possibly allow it to adjust the national strategy. It holds a specific position which enables it to more easily pursue its own goals which can then be passed onto other actors, and major governmental documents.

6. The DHS as an agenda-setter in the U.S. cyber security

As previously shown, the DHS has a special position in cyber security in the U.S., while its power in this area has been gradually enhanced through various policy directives. However, the scope of this power needs to be further examined and illustrated. Thus, this chapter analyzes the discourse of the DHS within the area of cyber security, and then later demonstrates whether its agenda-setting power allows it to push its own policies into the national cyber security strategy to frame cyberspace and cyber security. It focuses on the securitizing rhetoric within the documents of the DHS, or the ones it is associated with, to reveal if this department helps securitize cyber security and cyberspace in the U.S. For the discourse analysis, the thesis employs the political and Fairclough's discourse analysis together with Hansen and Nissenbaum's securitization theory which looks at various documents by the DHS itself, or the ones it cooperated on. This is crucial for determining whether the DHS aids with the ongoing securitization of the cyber security and cyberspace in the U.S., and if it gives a general idea of what kind of rhetoric appears in the documents it worked on. To demonstrate the agenda-setting power of the DHS, the findings from the first part of the chapter are compared to the national cyber security strategy of the U.S. to trace whether there is a similar rhetoric found in the first part.

6.1. The DHS and its perception of cyberspace

As previously mentioned, the DHS has been founded in 2002, under specific circumstances of the national tragedy which could have affected the way it treats its assigned tasks. Likewise, the department possesses more responsibilities and capabilities in cyber security than any other federal agency or executive branch department which makes it the leading actor in cyber security in the U.S. This was caused by the gradual delegation of powers in this respective area onto this department since its creation in 2002. Moreover, the securitizing discourse of cyberspace started before the establishment of the DHS, however, with the powers the department has in the area, it may be contributing to the ongoing securitization. Especially in last few years, cyber threats were always listed as one of the biggest threats to the U.S., including the report by various U.S. intelligence agencies (Miroff, 2018; Landay, 2018; Harris, 2019). Thus, it is important to identify whether there is a specific rhetoric towards cyberspace which could potentially allow to easily pass laws, bills, and other provisions that would not be able to be passed under 'regular' circumstances. In order to do that, the thesis attempts to reveal the securitizing discourse of the DHS in the area

of cyber security in several steps. First, the thesis analyzes seven documents both by the DHS and the ones it worked on. These documents were chosen based on their importance to the national strategy, the general public or the agency itself, their time relevance (their date of release does not exceed ten years so the data used is relevant), the topic relating to cyberspace, and diversity. To find the securitizing discourse outlined by Hansen and Nissenbaum, the thesis searches for three elements of securitization: hypersecuritization, technification, and every day security practices. It is relevant to look for them because they reveal the particular rhetoric that is specific for securitization of cyberspace, and better captures the construction of cyber threats which lie outsides the usually scope of this theoretical approach. To do that, it uses a computer software for qualitative analysis: Atlas.ti. It is able to create word count, relations between words, and based on the codes it can categorize data. For these reasons, it is a suitable program which can ease the process of discourse analysis, and highlight the hidden rhetoric within the documents. The method used is a combination of political discourse analysis and Fairclough's critical discourse analysis it allows to research to choose an analytical technique which is the most appropriate to it. Moreover, the thesis has demonstrated in the preceeding chapters the context, the evolution, and basis of the agenda-setting power of the DHS which is one of the important levels of the Fairclough's method. The thesis has also shown some of the documents in the historical context, in the relation towards the federal department, and other documents which in a way present interdiscursivity that is another level of the analysis used. The results of the first part are then compared to the National Cyber Strategy of the United States of America in order to find similarities and push of the agenda by the DHS into this document.

6.1.1. The DHS and its discourse in cyber security

For this analysis the thesis chose seven documents - U.S. Department of Homeland Security Cybersecurity Strategy (DHSCSS), Report to the President on Federal IT Modernization, Cyberspace Policy Review, Federal Cybersecurity Risk Determination Report and Action Plan, Addressing Urgent Cyber Threats to Critical Infrastructure, Homeland Security Information Network 2017 Annual Report, and Enabling Distributed Security in Cyberspace. After going through these documents, the conclusion will be presented whether the DHS helps continuation of the securitizing discourse. The stress is mostly put on the U.S. Department of Homeland Security Cybersecurity Strategy since it is one of the most important and recent documents released by the DHS, and thus, includes the most accurate data.

After running the word count analysis on all seven papers, the paper looks for three elements of securitization of cyber security. One of the most noticeable elements is hypersecuritization where the plausibility of a catastrophic event is securitized even though a situation like this has not happened before. Drawing up to the analysis, several points stand out in relation to hypersecuritization. The most repeated word in all of the documents is 'risk' (over 212 times throughout the seven documents), with other words such as 'threat' (over 103 times), 'threaten' (3 times), or 'harm' (9 times). This can be explained as creating a connection between cyber security and a dangerous uncertainty that could be brought upon the U.S. For illustration, in the opening statement of the U.S. Department of Homeland Security Cybersecurity Strategy, 'risk' appears 6 times, and the need for its better management, as well as greater dangers connected to the increased connectivity (DHS, 2018b, p. 1). Such an introduction immediately sets the idea of a cyberspace as a potential hazard which is then only deepened throughout the document. The Cyberspace Policy Review also stresses the exposure of the nation to cyber threats and its impact not only on the nation itself but also businesses, citizens, economy, and national security interests (DHS, 2009, p. 3; The White House, 2017, p. 17).

Moreover, the uncertainty of threats of cyberspace comes from all different types of actors including non-state actors, criminals, nations, or even terrorists (DHS, 2018b, p. 1-3). This brings to light another interesting link between cyber security and the types of actors using it. Words such as 'terrorist', 'criminals', 'criminal organizations', 'crime', 'terrorism' as well as the actors who are usually described as malicious, malevolent, threat actors or non-state exploiting cyberspace, and targeting the U.S. (DHS, 2018b, p. 1; DHS, 2009, p. 1; p. 3; NIAC, 2017, p. 27). This creates the illusion that cyberspace is full of 'hackers' whose only goal is to disrupt and hurt the nation, its citizens, and all sectors and industries. It also portrays these actors as 'sophisticated' which makes them seem more organized, dangerous and working with precision. Specifically naming the crimes such as cybercrime, cyber-attack, and especially terrorism resonates with everyone, and every sector since it is still one of the most feared events that could happen.

The DHS which is supposed to protect the nation against these dangers can cause concern by warning about them because if the agency that is supposed to tackle these issues is worried about them, then, it ultimately eases the process of securitization. The DHSCSS repeatedly emphasizes the growing capabilities of criminal actors and organizations, their skills that allow them to work under the radar, without leaving any trace (DHS, 2018b, p. 2, 15). Furthermore, it

adds up to the image of cyberspace which presents high levels of danger which could turn into a catastrophe. This is supported by the fact that the documents reflect on the possibility of catastrophic impact and consequences caused by cyber incidents, and especially in the DHSCSS which links it to better interconnectedness and the use of cyber in the area of essential services (DHS, 2018b, p. 1, 10; DHS, 2017a, p. 7; DHS, 2017b, p. 18). For example, Cyberspace Policy Review even mentions the potential crippling effects on society (DHS, 2009, p. 12). Moreover, the U.S. is described as vulnerable and exposed to these kinds of threats, and thus, there is an urgency to strengthen the resilience and protection (DHS, 2018b, p. 23; DHS, 2009, p. 11; DHS, 2011, p. 2; The White House, 2017, p. 2). The solution to this problem is often suggested in the documents, specifically, the federal government is seen as the one to tackle the problem, or as in the DHSCSS, the DHS is seen as the right agency to face the difficulties encompassed within the cyber security. By doing that, the government and the DHS reinforce their position as the best actors to resolve these matters. Likewise, the potential damage reaching 'catastrophic' levels implies the possible irreversible impact it may have on the nation, and every aspect of life. This step easies the legitimization of extreme measures because they are presented as critical for the survival of the country which can be often observed on the emphasis on the critical infrastructure and its resilience. Additionally, Cyberspace Policy Review points out the numerous intrusions cyberspace allows not only to the private and public sector but also people's lives (DHS, 2009, p. 13).

Another interesting aspect found throughout the documents is the use of terms relating to military, national security, law enforcement and intelligence such as 'cyber war', 'surveillance', 'defense'. Especially, Cyberspace Policy Review or even Report to President on Federal IT Modernization mention the use of all means necessary including the military means, as well as allowing protection of certain areas by the military (DHS, 2009, p. 4, 8, 23; DHS, 2017b, p. 39, 40). Likewise, it justifies the utilization of practices such as surveillance for purposes of protection (DHS, 2009, p. c-5). This can be an alarming process creating the illusion of the urgency of protection in return for giving up one's privacy to enhance the overall resilience. All of this supports the suggestion that the use of these terms helps adoption of special capacities (e.g. military) which allows for certain areas to be regulated by these bodies. But it also adds up to the negative perception of cyberspace and cyber security that is misleading and damaging, while also sparking up the fabricated need for additional protection. Despite these facts, it further suggests

that the reach of cyber goes into all the areas, and that nothing is excluded from it such as the national security, military, economy or political sector. Thus, it is apparent that elements of hypersecuritization occur in the documents by the DHS which incites to enhanced security, although no cyber incidents of such catastrophic scale, as it is emphasized, happened. Then, the perception of security is not only defined as national security, but it reaches to all the areas and sectors including economic, political, etc. This can also lead to an all-pervasive state of cyber-emergency where the powerful actors can constantly indicate the presence of threat, and thus, implement acts to diminish them. For instance, permitting surveillance is one of the measures creating the environment of permanent securitization. As people give up part of their privacy to gain the spurious feeling of protection, they are continuously reminded what could occur if they did not do that. Moreover, there is also a long-term impact where the effected entities accustom themselves to the new reality where they perceive it as normal like in the case of surveillance, that they have nothing to hide. This is a disturbing situation in which the norm in the society can change and become under control of the securitizing agents. Additionally, it can also alter the politics by the realization it could potentially pass and propose measures in the newly created environment, and thus, support and reinforce its existence. Ultimately, it can lead to the blurred lines between the internal and external security in which to provide domestic security, it may spill over to the external security. Under the exceptional circumstances, it may seem rational to pass these kind provisions that might conclusively affect the protection of for example citizens and businesses and combine it with the protection of the state and national security. For illustration, this could be the case of connecting the protection of cyberspace to terms relating to military. Especially, cyber security which is an all-encompassing field of different sectors can blur the lines easily, and change the distinction between the internal and external security.

Technification was present on a certain scale in all of the documents. This element provides a privileged position to experts in the field by highlighting the importance of a specific knowledge and expertise. The consequences can be far-reaching. For illustration, it creates a special discourse that is unique for cyber security, and lessen its approachability by other actors. Moreover, the particular role they are given, allows them to demonstrate this respective field, and thus, influence the discourse surrounding it, and even support its securitization. The call for ‘experts’, ‘knowledge’, or ‘specialized expertise’ appear in five out of the seven documents listed in the analysis. In the DHSCSS, the need for expertise is emphasized throughout the document which is

seen as a crucial measure for understanding cyber security and building important resilience structures (DHS, 2018b, p. 14). A similar sentiment is found throughout most of the documents which highlights the necessity of every agency and government to hire, train, and support cyber experts with a particular set of skills in order to increase the protection of all sectors including critical infrastructure, or prevent the possible catastrophic scenarios. In addition, the 'experts' are not limited to cyber but also from other areas such as legal, economic, or military. Their cooperation is important for the mitigation of evolving risks and threats. As demonstrated, the position of people with particular knowledge is lifted to a level that gives them a privileged position within the area. They are considered to be exceptional and essential for the protection of the country. Furthermore, the language used in the documents often involves specialized vocabulary for the field of cyber security and cyberspace such as 'binary', 'co-axial', 'dark web', 'encryption', or 'phishing'. For illustration, the NIAC report portrays past attacks by using this specialized vocabulary which can seem unimaginable to the general public (NIAC, 2017, p. 29). It creates an illusion that the problems regarding this area can be understood by a small group of people, while it further allows them to influence it. The experts possess the power to share their perception of cyberspace and cyber security to the public, and potentially support the securitization of the field. Thus, they may ultimately become the securitizing actors using their knowledge-based rhetoric in order to persuade the audience about the urgency of increased protection. It also makes it more difficult for 'regular people' to try to understand the issues, and possibly better comprehend the changes and problems mentioned in these documents. This gives more power to the DHS because it may then more easily justify certain changes within the field because it is hard to understand by the citizens. Therein, all the evidence suggests that technification also appears in the documents related to the DHS, while providing special status to experts from different fields which also limits the access to the area of cyber security.

While they are crucial for improving the protection of the country, innovating the field, or informing the public, their placement within the process need not to be dominating, and predominantly decisive (Moore, 2014, p. 50). Outside of the previously demonstrated consequences, it can also affect democratic processes and oversight. Taken the situation within the European Union Commission, it raises concerns that repercussions in this field might be similar. The Commission has been highly criticized for being dominated by limited number of experts that have been accused of creating closed system promoting technocratic policy-making, and

democratic deficit. By involving a small group of people it keeps exclusivity, gives control only to academia and industry. Although, the professionals tend to be from different sectors, the inclusivity may be limited, and exclude actors that might possess important insights (Moodie, Holst, 2014, p. 294, 300, 305). It can also ignore the gender and racial balance that may bring diverse backgrounds, and expand on new ideas. Moreover, as a whole, it may ultimately establish a non-transparent, restricted system which leads to a technocratic policy making (ibid, p. 305). That present problems for the democracy and oversight. This type of policy making allows 'technocrats' to make decisions that are not restricted by political processes, since they are at least partially removed from the public display. This also makes them less democratically accountable (Bangura, 2004, p. 1). Furthermore, it can limit the scope of political choices, and the final outcomes may become irrational (Moore, 2014, p. 53). The decisions can be made behind the closed doors which weakens the democratic process, accountability towards public, and additionally, it makes the oversight difficult. That is supported by the fact that the system can become opaque, exclusive, and inaccessible outside of the inner circle.

The last element – everyday security practice – is also one of the underlying themes of the documents. It links the citizens to the threat through forcing them to worry about their security so they get mobilized, involved and share the experiences of the threat. Especially 'civil liberties', 'civil rights', and 'privacy' are often emphasized as in need of upholding and protection in cyberspace (DHS, 2018b, p. 3; NIAC, 2017, p. 32; DHS, 2017b, p. 2). These resonate within the general public because they fall under the fundamental rights which are considered untouchable. The opening statements, and executive summaries often carry a message to the American people, the citizens, or the general public and their dependent relationship upon cyberspace, and the dangers that come with it (DHS, 2018b, p. 1; DHS, 2011, p. 2). Furthermore, the outreach of cyberspace transformed every sector and area, including daily lives which on one hand brought innovation and progress, on the other hand it brought risks that needed to be dealt with. (DHS, 2009, p. 22). Together with the previously mentioned affected sectors, it may give an idea that the potential threat may hit anyone, at any time, and thus, the proposed measures seem necessary. Additionally, it spreads fears about cyberspace and its effects on one's security, privacy, or even values since it may hurt the nation as well. It may then be used by the DHS to support their outlook on cyber security and facilitate the process of passing related legislation. Thus, there are apparent

everyday security practices within the discourse of the DHS that make citizens worried about the possible risks tied to cyberspace.

However, the securitizing actor needs to possess some securitizing power, or a political power in order to be able to securitize an issue. In reality it means that the actor needs to hold a certain position in the society which makes their statements seem more credible, and convincing, and therefore facilitate the passing of legislation. The most prominent actor in the documents is the DHS which is one of the most important federal departments in the U.S. Its special role in the federal system and its mission to protect the country give it a distinctive position in the society and provide it with securitizing power. Especially then in cyber security, the thesis demonstrated that with the evolution of the DHS, it gained more powers and responsibilities in cyber security until it became one of its core missions. Moreover, its cyber branch possesses the most capacities out of all federal departments and agencies which also enhances its overall standing, and powers in the field. All of these outlined points confirm the exceptional position of the DHS which grants it the required securitizing power it needs, while also augmenting its credibility. In its documents, the department tends to start its introduction by addressing the American people, or citizens, immediately referring to the problems within cyberspace, and the urgent call for immediate solutions. It demonstrates the ability of this federal department to better articulate successful security speech acts which have increased chances to end up in a legislation.

Nevertheless, two of the documents were initiated by the president of the U.S., or in cooperation with the NSC, and the HSC. Especially the presidents of the U.S. possess high levels of trustworthiness and credibility, as well as the White House itself and its staff. It is presumed that they have a wide range of information available, and thus know what the real threats are. Just like the DHS, the presidents set their opening statements that spark the need for immediate action in cyberspace, and the way it affects every part of people's lives (DHS, 2009, p. 1). Therein, the DHS in support of the other actors working on the documents presented in the chapter have the necessary securitizing power that allows them to be able to securitize their selected issues and areas. This is important for the persuasion of the audience to accept the 'dramatic' changes proposed by these bodies because they are convinced the adjustments are fundamental. At the same time, the DHS is portrayed as an agenda-setter but also an agent for presidency which adds to their dynamic.

As it was mentioned, securitization is a rhetorical act that allows for the acceptance of the extraordinary measures that could not be admitted under regular circumstances (Buzan et al., 1998). For an issue to be securitized, there has to be a securitizing actor (having a securitizing power) who presents a certain issue as an existential threat to the referent object (that is threatened by the issue), to the audience (its composition depends on the circumstances of the securitization) which needs to accept it as presented (Balzaq, Léonard, Ruzicka, 2016, p. 495-496). This can be identified in most of the DHS documents. The securitizing actor in this case is the DHS, or the DHS in cooperation with the presidents of the U.S., or other governmental bodies. They also suffice the requirement to possess securitizing power which was shown in the previous paragraph or retain political power that they possess by the nature of their existence. The issue presented by the actors is cyber security and cyberspace, supposedly posing an existential threat to not only the U.S. but also to its citizens, and every other part of the country. This establishes a collectivity of referent objects linking together all different parts of the nation and actors within in. Since the DHS, the presidents and other actors refer to the U.S. as being under the danger of inevitable risk, it also creates a situation where the securitizing actor overlaps with the referent object which increases the securitizing power of these actors. The threat comes from the 'sophisticated' hackers, nation-states, or even state actors who are trying to disrupt the functioning of the nation, stealing its sensitive data, money, or even attack the critical infrastructure that could ultimately paralyze the country.

The audience is mainly composed of citizens of the U.S., the government, but also to the allies of country. As demonstrated, most of the rhetoric is aimed at convincing and persuasion and the necessity for the acceptance of extraordinary measures. This is further captured by the emphasis on the technicality of the field which creates the illusion that it is only accessible to the experts and people possessing specialized knowledge. Based on the easy way of releasing these documents and passing the legislation, the audience may have accepted the proposed changes as legitimate, since there were almost no repercussions against it. However, this is difficult to substantiate. Furthermore, the three elements outlined by Hansen and Nissenbaum's securitization theory were also satisfied. The hypersecuritization plays an important role in all of the documents by securitizing a situation that has not occurred before, by highlighting its potential dangers, and by framing it within sectors such as the military or as an instance of high urgency and national security. Therefore, it is persuading its audience about the need to pass exceptional measures for

its protection, safeguarding the nation, and all of its parts. Then, technification has proven to be present as well, sparking to the paramount role of the experts, and the idea of the necessity of special knowledge and expertise in the area of cyber security, and cyberspace. It allows smaller group of people with these skills to control the field, and not have others try to join because they do not possess the required abilities or expertise. Lastly, everyday security practice also appeared in the documents, making citizens worried about the effects of cyberspace, their security, and pushing them to collectively share the common threat coming from this respective area. Thus, it can be concluded that the DHS is helping to continue with the securitizing discourse which started after the 9/11 and that is found throughout its documents.

6.2. Did the DHS push its own agenda onto the national cyber security strategy?

As mentioned, in 2018, President Donald Trump released the National Cybersecurity Strategy (NCS2018) which is the first document addressing this area in the past nine years. It sets the approach of the U.S. in the area of cyber security and cyberspace. However, with the powers of the DHS in this field, and the special relations there is between the president and the department, the question arises whether the DHS was able to push its own agenda and rhetoric into this document. Moreover, the DHSCSS and the NCS2018 were released only four months apart. The following part thus identifies whether there is a securitizing discourse found within the NCS2018, and if so, it will then be compared to the discourse and the agenda from the documents by the DHS which was examined in the previous chapter. In order to decide if this federal department influenced the national cyber security strategy, the thesis adapts the political agenda-setting theory. In this adaption, it would mean that the DHS is the department possessing the necessary powers to shape public opinion, push its own agenda onto other actors, or into certain documents, yet it might need the backing of policymakers. The particular policymaker in this situation can be the presidents of the U.S. who have had and still have a special relation with this department, and gradually assigned it more power over time. The president of U.S. holds a wide range of powers, some of them reaching to the legislative branch. The actor itself cannot make legislative proposals but he/she may influence with his/her statements, reports, State of the Union addresses, or threats of vetoing the legislation. Thus, the president can veto a bill which can be overridden by two-thirds vote in both of the chambers of Congress. Another option lies within the signing of the executive

order that is a directive of the president, and has the force of a law (U.S. Constitution, n.d.). In the process itself, there are several stages: agenda-setting, formulation-modification, adoption, and implementation. While the president is not directly involved it, it has been demonstrated that he/she influences in a way at every level (Gleiber, Shull, 1992, p. 464-465). Especially, in the initial stage provides the actor with a leadership with as a result of the unique position in national agenda setting (ibid, p. 443). Additionally, the theory also states that one political actor's agenda can be under the influence of another political actor (Van Aelst, Walgrave, 2006, p. 89). Hence, the same logic could be applied onto this case, where the agenda of the DHS could shape the national cyber security strategy. Likewise, the issues covered by media may be framed a particular way which then again could be applied to this particular case. The respective federal department could by its coverage of cyber security and cyberspace frame them in an exceptional securitizing manner, and thus, also affect the president and the NSC working on the national cyber security strategy.

6.2.1. The discourse within the National Cybersecurity Strategy of the United States

NCS2018 is the first national cyber security strategy document released in the last nine years which was a significant step for the Trump administration. It addresses a wide array of issues ranging from protection against cyber threats, lifting the position of the U.S. within the international cyber security area, the role and effectiveness of federal agencies, or the American economy (The White House, 2018, p. 3-5). It realizes the importance of cyberspace which brings innovation, but at the same time also risks that need to be mitigated. It also promotes the ongoing multi-stakeholder model of internet governance, secure internet and its freedom, or a cooperation with international partners (ibid, p. 24-25). More than any other document before, it stresses the need for protection of American people, economy, and it also leaves more room for private sector to get engaged (ibid, p. 10, 14, 15). It recognizes the long-term problem with the inadequate staffing of the cyber security professionals (ibid, p. 17) which has been one of the main critiques of the government. Moreover, it pledges to protect and invest into areas that have not been often mentioned before such as space, quantum technology (ibid, p. 15-16). This signals that the government realizes the raising importance of these fields but also the risks they may bring. To resolve the challenges and uphold the law, the strategy emphasizes the promotion of cyber norms, building cyber deterrence initiative, and using all instruments available (ibid, p. 21). Especially

this element, differs from the previous administrations because more than any other one before it admits the use of offensive cyber tools as counter measures. This is a major change in the stance of the government from the more defensive positions, towards the possibility of an actual counter-attack. Furthermore, just like the previous documents it stresses the need for increasing cyber resilience of critical infrastructure, cooperation of public and private sector, better funding, or protection of privacy (ibid, p. 6, 8, 24). Nevertheless, the whole strategy comes with a major issue – lack of necessary steps. While it outlines the general future approach of the government in many areas, it does not specify how it should be executed. It rarely mentions the agencies that could be responsible for carrying out outlined tasks. This is problematic because the missing details signify that the whole strategy is dependent on the willingness of Congress, private sector, or generally the government to take initiative, and start the process. If none of these do, the set out goals may never be fulfilled. In spite of that, it is an important document for the U.S. but also for its allies and the international community because not only does the national strategy address the significance of the cooperation with its partners but also the country is a leading actor in cyber security in the world. This can also mean that their approach in this respective area would be presented in international forums and international organizations, and could potentially be accepted as the norm for other countries. Compared to the other documents by the previous administrations, this one truly identifies the approach and the stance of the U.S. towards the cyber security and may be considered as the authoritative and superior document in comparison to previous ones.

Overall, while this national cyber security strategy may seem as a continuation of the policy set by the Bush and Obama administration, it goes at least one step further. Compared to its predecessors, it recognizes gaps and long-term problems such as lack of workforce, protection of new areas (space, quantum technology), or inadequate funding. Moreover, there is a shift of the U.S. towards a more pro-active offensive stance in cyberspace, emphasizing the upholding of norms and countering threats. Additionally, it leaves more open space for the initiative from the private sector to get involved. In other aspects, it continues with the existing policies including protection of critical infrastructure, cooperation with international allies, upholding internet freedom or protection of civil liberties. Nonetheless, it does not specify a way the strategy should be executed which may lead to a situation where it is never fulfilled. In the next section, the thesis attempts to find a securitizing discourse within this document which would demonstrate another

important stance of the government towards the cyber security. It also shows a deeper analysis of this paper, and illustrates additional important elements. It is then compared to the rhetoric found in the DHS documents which will show if this federal department pushed its agenda into the national strategy. In order to find out whether there is a securitizing discourse within this document, yet again, the securitization theory by Hansen and Nissenbaum is employed.

After running the analysis, it is immediately noticeable that there is rich evidence of hypersecuritization. One of the most noteworthy factors is the high frequency of words such as 'risk' (more than 30 times), 'threat' (over 30 times), 'threaten' (22 times), or 'harm' (4 times). Just like in the case of the DHS, it links the cyber security and cyberspace to unpredictability which can pose a potential danger to the U.S. For illustration, in the introduction of the document, the first paragraph alerts the American people about the new emerging threats coming from cyberspace (ibid, p. 1). It urgently warns about the dangers that are hidden within this area, gradually aggravates them throughout the paper, and suggests the demand for the measures to be taken. This is similar within the discourse set by the DHS which also tends to start the introductions with the demonstration of the hazards stemming from this field, and thus, establish the belief that there is a need for action. Moreover, the strategy urges for caution about the reach of cyber threats to supply chains, quantum computers, transportation, space, critical infrastructure, government, businesses, or even individuals (ibid, p. 16-19, 1). Therefore, the impact of an attack could affect not only the nation but also its businesses, citizens, economy, and many other areas. Furthermore, the endangerment stems from the actors imperiling the nation such as 'criminals' and 'criminal groups', 'rogue states', 'non-state actors', or 'terrorists' (ibid, p. 2, 10). Use of these words hints at the idea of cyberspace being driven by dangerous entities exploiting it for their own advantage, and threatening the U.S., its citizens, and its industries. Their activities are described as 'frequent', 'sophisticated' and 'malicious' which increases the fear surrounding this area because then they seem to be better organized and prepared to cause damage and disruption at any price. Yet again, the dangers such as 'cybercrime', 'cyber-attacks', or 'terrorism' are the main concerns (ibid, p. 24, 25), which facilitates the securitization since it creates a link between these activities and cyberspace. In this respect, the discourse is similar to the DHS.

However, there are slight differences. In the NCS2018, there are no direct mentions about hackers but there are only references to hacking. In addition, compared to the federal department, the national cyber security strategy explicitly names the states which conducted cyber-attacks, and

challenge the U.S. such as Russia, China, Iran, or North Korea (ibid, p. 1, 2). This is an interesting step which may also help securitization because by specifically naming adversaries, the threat actors are real, materialized, someone who the audience knows exists, and therefore, can fear. Nevertheless, it only expands on the actors that were outlined by the DHS and are then shared in this document which also emphasize their growing 'nefarious' capabilities (ibid, p. 2, 10). Although, the NCS2018 stresses the threats, and risks to every part of the nation, industry or sector, it does not link it to the catastrophic scenario but rather to a further escalation, costly consequences, or that the attack would come in times where the U.S. would not be far from the state of war (ibid, p. 2-3). This is a shift from the DHS rhetoric, nonetheless, the strategy overly emphasizes the damage that has been already done to the nation including violation of laws, espionage, intellectual property theft, system breaches, personal data breaches, or undermining democracy (ibid, p. 1-3). In a way, it still portrays the inevitable, catastrophic impact cyber incidents might have which corresponds to the DHS discourse. Additionally, the U.S. itself is on several accounts described as vulnerable to threats deriving from cyberspace while new vulnerabilities keep appearing which strikes the need for increasing resilience (ibid, p. 1, 3, 10). The U.S. government is proposed as the actor to deal with these issues, and the one to guarantee strengthening of cyber security and protection of the U.S. and American citizens (ibid, p. 6). Furthermore, it also appoints the DHS to secure the networks of federal agencies and the government excluding the DoD, to guide risk management in cyber security, or to oversee the management of cyber security personnel (ibid, p. 6, 7, 17). By doing this, the government bolsters its position as the main actor to tackle the problems in cyberspace but also the role of the DHS by delegating it the responsibility to secure the networks of the governmental. It further gives it a superior position in cyber security over other actors, and also consolidates its powers in this field.

Although, there are words relating to military including 'defense', or 'surveillance', they do not appear in such frequency as in the DHS documents. Despite that fact, the NCS2018 also stresses the need for updating the electronic surveillance, and its lawful use for gathering necessary evidence and information to disrupt criminal activity (ibid, p. 11). This yet again, legitimizes acquiring possibly private information, and technically giving up one's privacy in order to strengthen overall security. Additionally, the government is ready to deploy all instruments available such military (kinetic, cyber), financial, or law enforcement to prevent cyber incidents that could potentially hurt the U.S. and its allies (ibid, p. 21). The link between cyberspace and

national security capacities suggests that it is the entity that may be the best suited to help regulate it which has been brought to light before. Another similarity between the DHS discourse and the NCS2018 lies within the emphasis on the reach of cyber into all the area including economic, political, military, civil, or even private and public sectors. Therein, after presenting the evidence, it proves that hypersecuritization is present in the NCS2018, and aids to securitize against a catastrophic event that has not happened yet while also warning about the range of cyber threats. Moreover, the discourse found in this document about hypersecuritization elements is almost identical to the DHS discourse with only small deviations.

While technification factors occur in the document, they are manifested differently than in the DHS documents. The NCS2018 emphasizes the importance and need for 'knowledge' except this word only appears once (ibid, p. 10). It completely leaves out the word experts but instead of that calls for superior 'workforce', highly qualified 'professionals', and critical 'talent' (ibid, p. 17). These personnel are considered a national security advantage of the U.S. because the adversaries are also employing skilled professionals in order to hurt the nation. They are crucial for sustaining the competitiveness of the country, protecting it and its critical infrastructure, or leading innovation (ibid, p. 9, 17, 25). Thus, all sectors, businesses, and even federal government are advised to recruit, train, and develop skilled personnel to protect and mitigate risks in all the areas such as economic, law enforcement or political sectors. Therefore, similar to the DHS, it gives a special position to the qualified professionals who are an essential part in building cyber resilience, and ultimately have a privileged role in this field. As previously stated, it is necessary to include experts since they understand the systems protection the country, bring innovation, or creating guidance and frameworks. However, their position cannot be too powerful as it can lead to their domination. It may establish an exclusive, opaque, technocratic system which can be the least democratically and publicly accountable because the decisions are often excluded from the oversight (Bangura, 2004, p. 1; Moodie, Holst, 2014, p. 300, 305; Moore, 2014, p. 50). Moreover, the role allows them to present their vision of cyberspace and cyber security to the public that can ultimately make them securitizing agents themselves (Hansen, Nissembaum, 2009, p. 1165). Furthermore, it still uses specialized terms related to cyberspace and cyber security, more appropriate to this type of document, for example 'encryption', 'ICT', 'quantum', or 'botnets', but not in such quantity as the DHS. This is common again for both discourses, because it depicts cyber security as a field which can only be understood and managed by the people possessing

certain knowledge which ultimately gives them the power to influence it. The citizens and ordinary people then see the area as inaccessible, difficult to comprehend, which in turn facilitates the legislature and changes proposed by governmental and federal bodies. Along with this, the government and federal agencies and departments may effortlessly substantiate the proposed bills and amendments within cyberspace and cyber security because the citizens (who are usually part of the audience in securitization theory) do not understand the field based on the illusion of unattainable knowledge. In summary, all of these factors support the fact that there is a technification present within the NCS2018 which provides a special stature to qualified workforce in cyber security and limits its accessibility to other people. As for the similarity with the discourse by the DHS, there is a resemblance between the two, although, the vocabulary used in the national strategy has changed, yet the message within it is alike. Eventually, they both call for the urgency of retaining and recruiting skilled personnel as the crucial part of the protection of the nation, while they also use special terms even if not in the same frequency.

Compared to technification, the last element of Hansen and Nissenbaum's theory – everyday security practice – prevails. On multiple occasions, the document references to 'civil rights', 'civil liberties', or privacy' in relation to their need of protection and upholding them when conducting for example surveillance (ibid, p. 9, 21). Especially these areas are important for the citizens, and thus, their preservation may seem essential. Additionally, it may lead to easier acceptance of certain measures with the vision of enhanced protection of fundamental rights. Specifically, the NCS2018 delivers its message to the American people, fellow citizens, general public, and stresses their interconnectedness with cyberspace. On one hand, it shows it as an opportunity and great advancement necessary for prosperity, on the other hand, it exploits the threats that are hidden within it (ibid, p. 1). It is shown that the scope of cyberspace reaches to every sector, every part of the daily lives which are dependent on its functioning (ibid, p. 1-4). More than any other documents before, the national strategy emphasizes the word 'American' (45 times) or 'America' which creates collectivity, and the shared experience of these threats among all Americans. Yet again, by explicitly naming the group to which one could relate, it makes it easier to securitize since the hazard is better imaginable. All of these suggest that the danger could threaten anyone, especially Americans, their nation, and everything they stand for. It can then be used by the government or federal agencies and departments to pass extraordinary measures since they are believed to be crucial for the protection of everyone. The measures can range from

justification of surveillance, use of offensive cyber tools, allocation of resources for cyber security, to establishment of new departments. Therefore, it can be concluded that everyday security practice widely appears in the NCS2018, and helps spread the fear of potential risks among the general public. Additionally, there are similarities with the discourse outlined by the DHS, and on occasions is even more prominent and visible in the case of the national cyber security strategy.

Like in the previous case, the securitizing actor needs to hold a securitizing power, or retain political power which then authorizes him/her to be able to securitize a certain issue. There are two main actors in this document – the President of the U.S. and the NSC (which falls under the president). Referring to the earlier statement, the presidents of the U.S. hold high credibility and integrity, and they have the capability to enunciate successful speech acts that have increased chances to turn into a legislation. This is shown throughout the document where in the address to the Americans, it immediately sets cyberspace as an environment of malicious threats and risks, while also stressing the urgency for a solution and strengthened resilience (ibid, p. I). Likewise, the institutions related to presidents are considered to be well-informed and competent (e.g. the White House or the NSC) which raises their trustworthiness, and allows them to also successfully articulate speech acts. Therefore, the actors responsible for the national cyber security strategy possess the essential securitizing power which enables them to securitize particular issues and areas. It is substantial for the convincing of the audience so it is easier to accept the measures outlined in this particular document.

In this case however, it is also necessary to look at the external context under which the document was released. First, one of the major events that might have had an influence on the document has been the 2016 Russian interference in the U.S. presidential elections. It is one of the biggest cyber hacking incidents where Russia allegedly used fake social media accounts to make false posts, state-backed media which all led to an information warfare (Masters, 2018). The NCS2018 specifically names Russia as one of the perpetrators of reckless cyber-attacks against the nation. In the same year, China has been accused of cyber espionage on the U.S. which broke the cyber hacking deal, and also exploited data of almost 20 million people from the U.S. personnel office (Bing, Martina, 2018). This explains the explicit naming of the adversaries of the country, and the stress that is put on all different sectors including economic, military, or political. Additionally, in 2018, the DHS has concluded that the biggest threats to the U.S. are currently hacking and cyber-attacks, more than any other physical danger (Miroff, 2018). This supported

the sentiment that has been around cyberspace since the elections, where the wider public became aware of the risks lying within this area which then could have been used to further securitize it. Especially, the DHS could have influenced and pushed the president and the NSC into implementing its own agenda in the national security strategy since it appointed cyberspace as the biggest threat to the nation. On one hand, it is undeniable there is a high number of cyber-attacks against the systems in the country every day, on the other hand, the hazard could be exaggerated. The damage done is mostly economic, the democratic process, or espionage. While these are serious problems, they definitely are not the catastrophic events the DHS warned against. This may be downplaying the role of other threats, and underestimate the overall readiness. This federal department may have further used its special position in cyber security to encase its discourse into the NSC2018. This whole situation would also help explain why there might a prevailing securitizing discourse within this document.

Nonetheless, as previously stated, in order to securitize an issue, a securitizing actor presents an issue as an existential threat to the referent object, to an audience that needs to accept it as such (Balzaq, Léonard, Ruzicka, 2016, p. 495-496). These can be identified in this document as well. The securitizing actor is mainly the president in cooperation with the NSC, both of which satisfy the requirement of possessing the securitizing power (as demonstrated above), and retaining political power which they do since they are political and governmental entities. The issue presents cyberspace as a domain whose malicious risks pose an existential threat to the U.S., American people, its allies, its public and private sector. By specifically and continuously referring to the Americans, it is easier for the audience to imagine and feel the shared threat that could hit anyone, at any time. Moreover, by linking together all different parts of the country through the escalating danger, it creates the referent collectivity which then may facilitate the passing of the legislation. Likewise, the president and the NSC stress that the U.S. is at a big risk, just like the nation and the government (which they are part of), and it then establishes a condition under which the referent object partially overlaps with the securitizing actor. That ultimately increases the securitizing power of the securitizing actors, as well as their credibility in front of the audience since they are the ones to know when they are themselves at risk, while possessing the most knowledge. The danger comes from the ‘malicious’ non-state actors’, ‘rogue states’, ‘criminals’, and ‘terrorists’ who want to hurt the nation, exploit personal data, steal money from it and its business, or attack the democracy and the U.S. itself. The NCS2018 is addressed primarily to the American people,

but also the government, federal agencies, or public and private sector and the international allies. The whole document demonstrates the persuading rhetoric found in it, requesting the importance of the acceptance of extraordinary measures. Since the national cyber security strategy has been generally accepted after its release, it may be possible that the audience approved the amendments and propositions found within it. However, it may be too soon to tell. Additionally, it suffices three elements of securitization theory described by Hansen and Nissenbaum. First, the hypersecuritization aspects extensively appears throughout the document by warning against possible escalation, risks and threats stemming from cyberspace while linking it to national security. It constantly convinces the audience about the necessary exceptional measures that would increase the resilience of the nation, and everyone's within it. Second, the technification was found as well, although not in such frequency as in the case of the DHS. It suggested the superiority of the 'talent' and 'highly qualified workforce', while also sparking the idea of requiring special knowledge for even trying to comprehend cyber security and cyberspace. Then, everyday security practice is potentially the most prominent element spreading uncertainty among the citizens about their security, and the fear coming from cyberspace. Furthermore, it creates the referent collectivity which makes the ordinary people share the threat, and could force them to mobilize since they feel like they are threatened. Thus, the NCS2018 helps securitize the area of cyberspace and cyber security based on the analysis outlined above.

6.3. Is the cyber security agenda by the DHS present in the national cyber security strategy of the U.S.?

In the preceding sections, the thesis outlined the securitizing discourse found within seven documents by the DHS in the area of cyber security, as well as the securitizing discourse appearing in the national cyber security strategy of the U.S. where the main similarities and differences between the two were highlighted. In order to determine whether the DHS pushed its own agenda onto the national cyber security strategy, the political agenda-setting theory is used. Thus, the federal department would hold the necessary power that would allow it to shape public opinion, but also push its agenda onto other political actors, documents, frameworks, yet, only with the support of policymakers. In this case, it is the president of the U.S. who has a special relation with the department, assigned it more power over time, and was warned that the cyber threats are the biggest danger to the U.S. Additionally, the DHS could frame cyber security and cyberspace by

its coverage as dangerous and in need of extraordinary measures, and with that, further influence the president and the NSC that were at the time composing the national cyber security strategy.

In the analysis based on Hansen and Nissenbaum's securitization theory, the hypersecuritization elements were almost identical in the NCS2018 with the DHS. There were minor differences regarding the catastrophic scenarios, where the national cyber security strategy does not explicitly mention it, but rather stresses the possibility of a further escalation and damaging consequences. It also more frequently refers to the damage done to the U.S. such as the money loss, cyber espionage, or cyber-attacks conducted by other countries. Furthermore, it does not connect cyberspace to the military as much as the DHS, but still associates it with the national security of the U.S. Additionally, it specifically names the nations that attacked, or conducted cyber espionage on the U.S. In the other aspects including highlighting the risks hidden within cyberspace, the damage it could potentially do, its linkage to the national security, and the immediate necessary call for the measures to be taken in order to enhance resilience and ensure the security of the country, the discourses are interchangeable. Further, the DHS was assigned to secure the networks of federal agencies and government except the DoD, guide and lead risk management in cyber security, as well as management of cyber security workforce. This shows that yet again, this federal department has been chosen to take over more cyber security tasks which ultimately expands its power in the field.

As for the technification, it is present in both discourses but they differ in the use of words indicating the need for experts with specific knowledge. This is used in the DHS documents, whereas the NCS2018 calls for the qualified professionals, talent, or skilled workforce. However, it still shares the same message where it gives a superior position to people possessing specialized knowledge in cyber security since it creates the illusion that they are the only ones who can properly understand it, and tackle its problems. It also allows a small group of people to influence the field, and thus, facilitate taking control over it. Another aspect, which is identical for both discourses, is the use of technical, specialized terms related to cyberspace and cyber security, although they are different throughout the documents. Therefore, even if there is a different vocabulary, the technification is still obvious in both of the discourses which ultimately share the same idea behind their rhetoric, and therein are similar.

In the case of the everyday security practice, it is manifested in both of the discourses, in almost identical manner. In the national cyber security strategy, it is however more prominent and

frequent than in the one by the DHS. They highlight the dangers of cyberspace, the need of enhanced protection and upholding of the fundamental rights. Moreover, they also excessively address the American people, citizens, or the allies. All of these lead to the shared experience of threat, and then potential mobilization.

Based on the outlined evidence, it is concluded that the discourse within the national cyber security strategy corresponds to the one by the DHS. On top of that, in 2018, the DHS highlighted the cyber threats, especially hacking and cyber-attacks, as the biggest threat to the U.S., warning against online attack of a magnitude of the 9/11 (Miroff, 2018). This rhetoric reflected the fears surrounding cyberspace since 2016 elections that stirred uncertainty of risks within the general public which in turn helps the securitization of the field. Through this way, the DHS also pushed its agenda onto the NCS2018, and thus, the national cyber security strategy of the U.S. After taking into account all the factors and evidence presented, the DHS was able to influence the national cyber security strategy of the U.S., successfully use its powers in the area of cyber security, and maximize its privileged relation with powerful policymakers for its profit. It ultimately increased its powers in this respective area but also its overall position within the federal agencies.

Conclusion

The national security-focused approach of the U.S. towards cyber security, and the position of the DHS within it, present an interesting reality. This thesis revealed that the DHS used its influence to put its discourse into the national cyber security strategy. It further analyzed the cyber security strategy of the U.S., while also determining that there has been a securitization of this field after 9/11.

The DHS was chosen as a case study based on its wide array of tasks and capabilities in cyber security, which makes it a leading federal department in this area. Also, its responsibility to provide national security to the U.S. grants it special agenda-setting powers in the security field. Ultimately, it revealed the presence of securitizing discourse in the cyber security strategy of the U.S., and by employing process tracing on the events of 9/11, it provided an explanation for the specific stance of the U.S. towards the cyber security. Additionally, this thesis outlined the evolution of the field in relation to the DHS, its privileged position and internal structure focusing on cyber security, its agenda-setting powers, and its impact on the national cyber security strategy.

First, the thesis specified the theoretical approach of securitization theory, its modified approach by Hansen and Nissenbaum, as well as agenda-setting theory, specifically political agenda setting. In terms of the theoretical debates, the thesis contributed to the securitization theory since the modification by Hansen and Nissenbaum shows the agenda-setting powers of actors by demonstrating their interpretation of threats, and framing of cyberspace. However, it does not explain how these actors can push their policies, ideas or discourse onto other actors. To solve this issue, the thesis expanded the modified approach by elements of political agenda setting theory which provided an illustration and clarification of such actions, while also revealing the securitizing power the actors possess. Moreover, it widened the scope of securitizing actors to new, previously inadequately studied ones such as the federal agencies and departments (e.g. the DHS). It further presented key terms used in the work - cyberspace and cyber security – which signified the importance and problematic nature of the respective topics. Then, it proposed a methodology encompassing political discourse analysis and Fairclough's critical discourse analysis, historical analysis, and process tracing. By employing all three analytical approaches and a combination of different research methods, the contribution of the thesis is that it facilitated the triangulation of data through cross verification from multiple sources. While political and critical discourse analysis identified the securitizing rhetoric and influence of political actors, historical analysis and

process tracing helped explain the context of the securitization, historical base, and structural conditions of the stance of the U.S. towards cyber security.

Consequently, the operationalization explained the way the thesis utilized data and literature, and how it proceeded with the analysis. The following literature review identified a wide range of topics concentrating on cyber security in the U.S., however, they were mostly focused around national security, the military, terrorism, or securitization of the field. Compared to other actors such as the EU, the U.S. has a more national security-focused approach, which was the main reason for considering only literature regarding cyber security in the context of the U.S. It further revealed and recognized the gap in the literature concentrating on the position of the federal agencies and departments in cyber security, since they perform most of the cyber related tasks, and hold a leading role in the field.

The next chapter introduced the historical analysis and evolution of the DHS and cyber security before and after 9/11. Initially, it discovered that from the moment of the establishment of the DHS, it has been tasked with information analysis and infrastructure protection, which has progressively expanded to cyber security and cyberspace. Moreover, its primary role and mission of providing protection for the homeland led to a treatment of cyberspace as one of its components. Its perception of cyberspace as a potential national security threat reflected this, and ultimately prompted the use of tools related to the protection of the nation, although, in certain cases (e.g. digital economy), other instruments would be more appropriate. Additionally, cyberspace has been perceived as a potential danger since the Reagan administration, yet, the events of 9/11 served as a securitizing moment because terrorists executed it.

The chapter further included the process tracing test – the Smoking Gun – based on the outlined historical evidence, and determined if there has been a securitization of cyberspace and cyber security after 9/11. It concluded that the events of 9/11 served as a catalyst moment that can be traced back to the Reagan era where concerns about cyberspace were first publicly voiced. The succeeding administrations stuck to the same rhetoric, which only changed with new technologies. Yet, the findings substantiate the assumption that the first opportunity to securitize the field opened with the 9/11 events rounding off the ongoing discourse from 1980s. It also legitimized the urgent call for the establishment of a homeland security department which became the DHS. After the events, the subsequent administrations sustained similar securitizing approaches, concentrating on

expanding cyber resilience and transforming with technological advancements, with each adding slight nuances in the field.

In addition, with each new administration, the DHS has been assigned more responsibilities and capacities in cyber security, which granted it a leading position over other government organizations. It then further demonstrated the privileged position of this federal department by describing the internal structure of its cyber security branch – CISA. It showed the large reach of this division into various areas, a link between critical infrastructure and cyber security, and the extensive responsibilities and capacities this agency has. The chapter also indicated the position of other federal agencies in the executive branch – FBI, NSA, DoD – in cyber security. It substantiated the assumptions that the DHS is a privileged actor in the field, since it is tasked with and given most of the assignments and capabilities. However, together all the agencies created a complex front of defense against cyber threats which is a necessary element in the age of swiftly rising technological problems.

In the last chapter, the thesis assessed the agenda-setting power of the U.S., and the approach of the U.S. in cyber security. It used a political discourse analysis and Fairclough's critical discourse analysis whose levels have been demonstrated throughout the thesis by demonstrating context, historical evolution, the DHS, and some of the documents in relation to cyber security or one another etc. In terms of empirical findings, the thesis' contribution lies in uncovering that the discourse found in seven documents by the DHS fulfilled the securitizing criteria. Moreover, the discourse also met the three elements outlined by Hansen and Nissenbaum, and thus it concluded that the DHS maintained a securitizing rhetoric in cyber security, supporting the existence of this discourse since 9/11. As for the national cyber strategy, while it may have seemed a pure continuation of existing policies, it progressed further and recognized the ongoing problems within the field, the need for a comprehensive strategy, and expanded into new, overlooked fields. However, it does not specify the particular steps for how the strategy should be executed, which leads to a situation where it is left unfulfilled in the future. Furthermore, the thesis found strong correlations the securitizing elements found in the National Cybersecurity Strategy of the United State of America corresponded to the ones present in the documents by the DHS. Thus, it concluded that the DHS has successfully utilized its agenda-setting powers, exposed throughout the thesis, and used its influence to include its ideas and policies on the national level.

Developing the national cyber security strategy was a major, essential step in this area for the U.S. However, the gaps that were identified need to be resolved. While the strategy is important, without a proper execution it would just be empty words that would leave the country behind the fast pace of technological progress. In this case, it might truly open a window of opportunity for adversaries to threaten the U.S., and other competitors to claim the leading position in cyberspace. Nonetheless, the fact that it was influenced by one of its own actors has important implications, and demonstrates the main contribution of the thesis. Initially, it proves that federal agencies and departments possess agenda-setting power in areas such as cyber security, and that they are not just mere advisors, defenders, or agents for the government. The DHS has its own policies, objectives and perceptions that inevitably get transferred to other actors based on its position and influence. It could make the government more aware of what they decide to include in their documents and strategies focusing on cyber security. It also points to the fact that none of the actors in the field should be underestimated.

The securitization of cyber security after 9/11 shows a culmination of long-term rhetoric that consolidated the approach towards it for years to come. It is supported by various actors, including the DHS, which only help its continuation, and ultimately justify use of measures (e.g. surveillance) which could have abiding implications on society, democracy, or the country itself. The linking of national security and military tools to cyberspace can also prevent application of more suitable instruments to deal with risks within it.

Nevertheless, the scope of the thesis still only concentrates on the position of one federal department in the cyber security arena. It could have even reflected its discourse onto other actors such as the other branches of the government or the public sector. Although the DHS possesses the most agenda-setting power, other departments also have influence. For example, the DoD also holds a strong position in the field. The securitization and its implications could go even more in depth, and have different effects on undisclosed areas. That of course signifies the need for additional research to be done in cyber security as it promptly expands to new fields and augments its importance.

List of References

Amirian, M.R., Rahimi, A. and Sami, G., 2012. A Critical Discourse Analysis of the Images of Iranians in Western Movies: The Case of Iranium. *International Journal of Applied Linguistics and English Literature*, *1*(5), pp.1-13.

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

Bandyopadhyay, L., 2001, in Cordesman, A.H. and Cordesman, J.G., 2002. *Cyber-threats, information warfare, and critical infrastructure protection: defending the US homeland*. Greenwood Publishing Group.

Bangura, Y., 2004. Technocratic Policy Making and Democratic Accountability. UNRISD Research and Policy Brief, 3(1), pp.1-4.

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

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

BBC News. (2014). How the US spy scandal unravelled. [online] Available at: https://www.bbc.com/news/world-us-canada-23123964 [Accessed 6 Mar. 2019].

Bendrath, R., Eriksson, J. and Giacomello, G., 2007. From'cyberterrorism'to'cyberwar', back and forth. *International Relations and Security in the Digital Age. Hrsg. von Johan Eriksson und Giampiero Giacomello. Abingdon: Routledge*, pp.57-82.

Bendrath, R., Eriksson, J. and Giacomello, G., 2007. From'cyberterrorism'to'cyberwar', back and forth. International Relations and Security in the Digital Age. Hrsg. von Johan Eriksson und Giampiero Giacomello. Abingdon: Routledge, pp.57-82.

Bennett, A., 2010. Process tracing and causal inference.

Betz, D.J. and Stevens, T., 2013. Analogical reasoning and cyber security. *Security Dialogue*, *44*(2), pp.147-164.

Bing, C. and Martina, M. (2018). U.S. accuses China of violating bilateral anti-hacking deal. [online] Reuters. Available at: https://www.reuters.com/article/us-usa-china-cyber-idUSKCN1NE02E [Accessed 9 Apr. 2019].

Borja, E.C., 2008. Brief Documentary History of the Department of Homeland Security, 2001-2008. US Department of Homeland Security, History Office.

Buzan, B., Wæver, O. and De Wilde, J., 1998. *Security: a new framework for analysis*. Lynne Rienner Publishers.

Cavelty, M.D., 2008. Cyber-terror—looming threat or phantom menace? The framing of the US cyber-threat debate. *Journal of Information Technology & Politics*, *4*(1), pp.19-36.

Cavelty, M.D., 2008. Cyber-terror—looming threat or phantom menace? The framing of the US cyber-threat debate. Journal of Information Technology & Politics, 4(1), pp.19-36.

Chairman and Ranking Member Subcommittee on Cybersecurity, Science, and Research & Development of the U. S. House of Representatives Select Committee on Homeland Security (2004). Cybersecurity for the Homeland [online] Available at: https://www.hsdl.org/?view&did=479978 [Accessed 5 Mar. 2019]

Christou, G., 2017. The EU's Approach to Cybersecurity.

Cobb, R.W. and Elder, C.D., 1971. The politics of agenda-building: An alternative perspective for modern democratic theory. *The Journal of Politics*, *33*(4), pp.892-915.

Collier, D., 2011. Understanding process tracing. PS: Political Science & Politics, 44(4), pp.823-830.

Collier, D., 2011. Understanding process tracing. *PS: Political Science & Politics*, *44*(4), pp.823-830.

Condron, S.M., 2006. Getting it right: Protecting American critical infrastructure in cyberspace. *Harv. JL & Tech.*, *20*, p.403.

Cordesman, A.H. and Cordesman, J.G., 2002. *Cyber-threats, information warfare, and critical infrastructure protection: defending the US homeland*. Greenwood Publishing Group.

Dearing, J.W. and Rogers, E., 1996. *Agenda-setting* (Vol. 6). Sage publications.

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

Denning, D.E.R., 1999. *Information warfare and security* (Vol. 4). Reading, MA: Addison-Wesley.

Department of Defense (2018). Summary Department of Defense Cyber Strategy. [online] Available at: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF [Accessed 16 Mar. 2019].

Department of Homeland Security (DHS) (2009). Cyberspace Policy Review. [online] Available at: https://www.dhs.gov/publication/2009-cyberspace-policy-review [Accessed 5 Mar. 2019]

Department of Homeland Security (DHS) (2009). Cyberspace Policy Review. [online] Available at: https://www.dhs.gov/publication/2009-cyberspace-policy-review [Accessed 9 April 2019]
Department of Homeland Security (DHS) (2011). Enabling Distributed Security in Cyberspace. [online] Available at: https://www.dhs.gov/enabling-distributed-security-cyberspace [Accessed 9 April 2019]
Department of Homeland Security (DHS) (2017). HSIN 2017 Annual Report. [online] Available at: https://www.dhs.gov/hsin-2017-annual-report [Accessed 9 April 2019] A
Department of Homeland Security (DHS) (2017). Report to President on Federal IT Modernization. [online] Available at: https://itmodernization.cio.gov/ [Accessed 9 April 2019] B
Department of Homeland Security (DHS) (2018). U.S. DEPARTMENT OF HOMELAND SECURITY CYBERSECURITY STRATEGY. [online] Available at: https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf [Accessed 5 Mar. 2019]
Department of Homeland Security (DHS) (2018). U.S. DEPARTMENT OF HOMELAND SECURITY CYBERSECURITY STRATEGY. [online] Available at: https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf [Accessed 9 April 2019]
Department of Homeland Security (DHS). (2018). Cyber Storm: Securing Cyber Space. [online] Available at: https://www.dhs.gov/cyber-storm [Accessed 5 Mar. 2019]. A
Department of Homeland Security (DHS). (n.d.). About CISA. [online] Available at: https://www.dhs.gov/cisa/about-cisa [Accessed 16 Mar. 2019]. A
Department of Homeland Security (DHS). (n.d.). Continuous Diagnostics and Mitigation. [online] Available at: https://www.dhs.gov/cisa/cdm [Accessed 16 Mar. 2019]. F
Department of Homeland Security (DHS). (n.d.). Critical Infrastructure Sectors. [online] Available at: https://www.dhs.gov/cisa/critical-infrastructure-sectors [Accessed 16 Mar. 2019]. O
Department of Homeland Security (DHS). (n.d.). Cross Sector Risk Management. [online] Available at: https://www.dhs.gov/cisa/cross-sector-risk-management [Accessed 16 Mar. 2019].Q
Department of Homeland Security (DHS). (n.d.). Election Security. [online] Available at: https://www.dhs.gov/topic/election-security [Accessed 16 Mar. 2019]. W

Department of Homeland Security (DHS). (n.d.). Emergency Communications Division. [online] Available at: https://www.dhs.gov/cisa/emergency-communications-division [Accessed 16 Mar. 2019]. H

Department of Homeland Security (DHS). (n.d.). Enhanced Cybersecurity Services (ECS). [online] Available at: https://www.dhs.gov/cisa/enhanced-cybersecurity-services-ecs [Accessed 16 Mar. 2019]. E

Department of Homeland Security (DHS). (n.d.). Federal Network Resilience. [online] Available at: https://www.dhs.gov/cisa/federal-network-resilience [Accessed 16 Mar. 2019]. D

Department of Homeland Security (DHS). (n.d.). FPS What We Do: FPS Services. [online] Available at: https://www.dhs.gov/fps-what-we-do-fps-services [Accessed 16 Mar. 2019]. P

Department of Homeland Security (DHS). (n.d.). Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force. [online] Available at: https://www.dhs.gov/cisa/information-and-communications-technology-ict-supply-chain-risk-management-scrm-task-force [Accessed 16 Mar. 2019]. S

Department of Homeland Security (DHS). (n.d.). Infrastructure Information Collection Division. [online] Available at: https://www.dhs.gov/cisa/iicd [Accessed 16 Mar. 2019]. J

Department of Homeland Security (DHS). (n.d.). Infrastructure Security Division. [online] Available at: https://www.dhs.gov/cisa/infrastructure-security-division [Accessed 16 Mar. 2019].I

Department of Homeland Security (DHS). (n.d.). Infrastructure Security Compliance Division. [online] Available at: https://www.dhs.gov/cisa/iscd [Accessed 16 Mar. 2019]. K

Department of Homeland Security (DHS). (n.d.). National Critical Functions Initiative. [online] Available at: https://www.dhs.gov/cisa/national-critical-functions-initiative [Accessed 16 Mar. 2019]. T

Department of Homeland Security (DHS). (n.d.). National Cybersecurity & Communications Integration Center. [online] Available at: https://www.dhs.gov/cisa/national-cybersecurity-communications-integration-center [Accessed 16 Mar. 2019]. B

Department of Homeland Security (DHS). (n.d.). National Cybersecurity Protection System (NCPS). [online] Available at: https://www.dhs.gov/cisa/national-cybersecurity-protection-system-ncps [Accessed 16 Mar. 2019]. G

Department of Homeland Security (DHS). (n.d.). National Infrastructure Coordinating Center. [online] Available at: https://www.dhs.gov/cisa/national-infrastructure-coordinating-center [Accessed 16 Mar. 2019]. L

Department of Homeland Security (DHS). (n.d.). Pipeline Cybersecurity Initiative. [online] Available at: https://www.dhs.gov/cisa/pipeline-cybersecurity-initiative [Accessed 16 Mar. 2019].U

Department of Homeland Security (DHS). (n.d.). Protective Security Coordination Division. [online] Available at: https://www.dhs.gov/cisa/protective-security-coordination-division [Accessed 16 Mar. 2019]. M

Department of Homeland Security (DHS). (n.d.). Sector Outreach and Programs Division. [online] Available at: https://www.dhs.gov/cisa/sopd [Accessed 16 Mar. 2019]. N

Department of Homeland Security (DHS). (n.d.). Stakeholder Engagement and Cyber Infrastructure Resilience. [online] Available at: https://www.dhs.gov/cisa/stakeholder-engagement-and-cyber-infrastructure-resilience [Accessed 16 Mar. 2019]. C

Department of Homeland Security (DHS). (n.d.). Tri-Sector Executive Working Group. [online] Available at: https://www.dhs.gov/cisa/tri-sector-executive-working-group [Accessed 16 Mar. 2019]. V

Department of Homeland Security (DHS). n.d. *Overview.* [online] Available at: https://www.dhs.gov/topic/overview [Accessed 2 Mar. 2019] W

Department of Homeland Security. (DHS) (2019). CISA. [online] Available at: https://www.dhs.gov/CISA [Accessed 6 Mar. 2019].

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

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

Dunn, M.A., 2007. *Cyber-security and threat politics: US efforts to secure the information age*. Routledge.

Embar-Seddon, A., 2002. Cyberterrorism: Are we under siege?. *American Behavioral Scientist*, *45*(6), pp.1033-1043.

Eriksson, J. and Giacomello, G., 2007. Closing the Gap Between International Relations Theory and Studies of Digital Age Security.

Eriksson, J., 2001. Cyberplagues, IT, and security: Threat politics in the information age. *Journal of Contingencies and Crisis Management*, *9*(4), pp.200-210.

Eriksson, Johan. (2001). Securitizing IT. 145-163.

European Commision, 2013. 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

Fairclough, N., 2001. Critical discourse analysis as a method in social scientific research. Methods of critical discourse analysis, 5, pp.121-138.

Fairclough, N., 2003. Analysing discourse: Textual analysis for social research. Psychology Press.

Fairclough, N., 2013. Critical discourse analysis: The critical study of language. Routledge.

Federal Bureau of Investigation (FBI). (n.d.). Addressing Threats to the Nation's Cybersecurity. [online] Available at: https://www.fbi.gov/file-repository/addressing-threats-to-the-nations-cybersecurity-1.pdf/view [Accessed 16 Mar. 2019]. A

Federal Bureau of Investigation (FBI). (n.d.). Cyber Crime. [online] Available at: https://www.fbi.gov/investigate/cyber [Accessed 16 Mar. 2019]. B

Federal Bureau of Investigation (FBI). (n.d.). National Cyber Investigative Joint Task Force. [online] Available at: https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force [Accessed 16 Mar. 2019]. C

Federation of American Scientists (2012). Presidential Policy Directive - 20. [online] Available at: https://fas.org/irp/offdocs/ppd/ppd-20.pdf [Accessed 5 Mar. 2019]

Federation of American Scientists. (1984). National Security Decision Directive Number 145 National Policy on Telecommunications and Automated Information Systems Security. [online] Available at: https://fas.org/irp/offdocs/nsdd145.htm [Accessed 5 Mar. 2019].

Federation of American Scientists. (1997). CRITICAL FOUNDATIONS PROTECTING AMERICA'S INFRASTRUCTURES: The Report of the President's Commission on Critical Infrastructure Protection. [online] Available at: https://fas.org/sgp/library/pccip.pdf [Accessed 5 Mar. 2019].

Fischer, E.A., 2005, February. Creating a national framework for cybersecurity: An analysis of issues and options. LIBRARY OF CONGRESS WASHINGTON DC CONGRESSIONAL RESEARCH SERVICE. [online] Available at https://fas.org/sgp/crs/natsec/RL32777.pdf [Accessed 5 Mar. 2019]

Frohmann, B., 1992. The power of images: a discourse analysis of the cognitive viewpoint. *Journal of documentation*, *48*(4), pp.365-386.

Furnell, S.M. and Warren, M.J., 1999. Computer hacking and cyber terrorism: The real threats in the new millennium?. *Computers & Security*, *18*(1), pp.28-34.

Gartzke, E., 2013. The myth of cyberwar: Bringing war in cyberspace back down to earth. *International Security*, *38*(2), pp.41-73.

Gasper, P.D., 2008. Cyber threat to critical infrastructure. *Idaho National Laboratories http://usacac. army. mil/cac2/cew/repository/presentations/15_Idaho_Natl_Lab_IACS-CI_Threat_2010-2015. pdf Accessed*, *22*, p.2012.

Gee, J.P., 2004. *An introduction to discourse analysis: Theory and method*. Routledge.

Geers, K., 2009. The cyber threat to national critical infrastructures: Beyond theory. *Information Security Journal: A Global Perspective*, *18*(1), pp.1-7.

Gjelten, T., 2013. First strike: US cyber warriors seize the offensive. *World Affairs*, pp.33-43.

Gleiber, D.W. and Shull, S.A., 1992. Presidential influence in the policymaking process. Western Political Quarterly, 45(2), pp.441-467.

Glen, C. (2014). *Internet Governance: Territorializing Cyberspace?*. Politics & Policy, [online] 42(5), pp.635-657. Available at: http://eds.a.ebscohost.com/eds/pdfviewer/pdfviewer?vid=1&sid=7d6d9ed6-c883-4459-b328-8c553c71f2d4%40sessionmgr4010

Greenwald, G. and MacAskill, E. (2013). Obama orders US to draw up overseas target list for cyber-attacks. [online] the Guardian. Available at: https://www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas [Accessed 6 Mar. 2019].

Hajer, M. and Versteeg, W., 2005. A decade of discourse analysis of environmental politics: Achievements, challenges, perspectives. *Journal of environmental policy & planning*, *7*(3), pp.175-184.

Hansen, L. and Nissenbaum, H., 2009. Digital disaster, cyber security, and the Copenhagen School. *International studies quarterly*, *53*(4), pp.1155-1175.

Hansen, L. and Nissenbaum, H., 2009. Digital disaster, cyber security, and the Copenhagen School. *International studies quarterly*, *53*(4), pp.1155-1175.

Hansen, L. and Nissenbaum, H., 2009. Digital disaster, cyber security, and the Copenhagen School. International studies quarterly, 53(4), pp.1155-1175.

Harris, S. (2019). Testimony by intelligence chiefs on global threats highlights differences with president. [online] The Washington Post. Available at: https://www.washingtonpost.com/world/national-security/intelligence-officials-will-name-biggest-threats-facing-us-during-senate-hearing/2019/01/28/f08dc5cc-2340-11e9-ad53-824486280311_story.html?utm_term=.6308e415e810 [Accessed 10 Apr. 2019].

Harrop, W. and Matteson, A., 2015. Cyber resilience: A review of critical national infrastructure and cyber-security protection measures applied in the UK and USA. In *Current and Emerging Trends in Cyber Operations* (pp. 149-166). Palgrave Macmillan, London.

Hern, A. (2017). WannaCry, Petya, NotPetya: how ransomware hit the big time in 2017. [online] the Guardian. Available at: https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware [Accessed 6 Mar. 2019].

Hilgartner, S. and Bosk, C.L., 1988. The rise and fall of social problems: A public arenas model. *American journal of Sociology*, *94*(1), pp.53-78.

Howe, G.F., 1974. The early history of NSA. Cryptologic Spectrum, 4(2), pp.11-17.

International Telecommunication Union. n.d.. *Cybersecurity*. [online] Available at: https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

Johnstone, B., 2018. *Discourse analysis* (Vol. 3). John Wiley & Sons.

Joint Chief of Staff (1998). Joint Doctrine for Information Operations. [online] Available at: http://www.c4i.org/jp3_13.pdf , [Accessed 15 March 2019]

Jørgensen, M.W. and Phillips, L.J., 2002. *Discourse analysis as theory and method*. Sage.

Kaiser, Frederick m., 2005, United States Homeland Security: Interagency Coordination and Concerns. Conference Papers -- International Studies Association [online]. pp. 1-15, [Accessed 6 February 2019].

Kang, C. and Frenkel, S. (2018). Facebook Says Cambridge Analytica Harvested Data of Up to 87 Million Users. [online] New York Times. Available at: https://www.nytimes.com/2018/04/04/technology/mark-zuckerberg-testify-congress.html [Accessed 16 Mar. 2019].

Kapto, A.S., 2013. Cyberwarfare: Genesis and doctrinal outlines. Herald of the Russian Academy of Sciences, 83(4), pp.357-364.

Kenney, M., 2015. Cyber-terrorism in a post-stuxnet world. *Orbis*, *59*(1), pp.111-128.

Kuehl, D.T., 2009. From cyberspace to cyberpower: Defining the problem. *Cyberpower and national security*, *30*.

Kundnani, A., 2004. Wired for war: military technology and the politics of fear. Race & class, 46(1), pp.116-125.

Lachow, I., 2009. Cyber terrorism: Menace or myth. *Cyberpower and national security*, pp.434-467.

Landay, J. (2018). U.S. intel chief warns of devastating cyber threat to U.S. infrastructure. [online] Reuters. Available at: https://www.reuters.com/article/us-usa-russia-cyber-coats/u-s-intel-chief-warns-of-devastating-cyber-threat-to-u-s-infrastructure-idUSKBN1K32M9 [Accessed 10 Apr. 2019].

Lawson, S., 2012. Putting the "war" in cyberwar: Metaphor, analogy, and cybersecurity discourse in the United States. *First Monday*, *17*(7).

Lawson, S.T., Yeo, S.K., Yu, H. and Greene, E., 2016, May. The cyber-doom effect: The impact of fear appeals in the US cyber security debate. In *Cyber Conflict (CyCon), 2016 8th International Conference on* (pp. 65-80). IEEE.

Lewis, J., 2003. Cyber terror: Missing in action. *Knowledge, Technology & Policy*, *16*(2), pp.34-41.

Lewis, J.A., 2002. *Assessing the risks of cyber terrorism, cyber war and other cyber threats*. Washington, DC: Center for Strategic & International Studies.

Lewis, J.A., 2005. Aux armes, citoyens: Cyber security and regulation in the United States. *Telecommunications Policy*, *29*(11), pp.821-830.

Lewis, J.A., 2008. Holistic Approaches to Cybersecurity to Enable Network Centric Operations. *statement before Armed Services Committee, Subcommittee on Terrorism, Unconventional Threats and Capabilities, 110th Cong., 2nd sess*, *1*.

Lewis, T.G., 2014. *Critical infrastructure protection in homeland security: defending a networked nation*. John Wiley & Sons.

Lindsay, J.R., 2013. Reinventing the Revolution: Technological Visions, Counterinsurgent Criticism, and the Rise of Special Operations. Journal of Strategic Studies, 36(3), pp.422-453.

Luo, X. and Liao, Q., 2007. Awareness education as the key to ransomware prevention. Information Systems Security, 16(4), pp.195-202.

Lynn, W.J., 2010. Defending a new domain: the Pentagon's cyberstrategy. *Foreign Affairs*, *89*(5), pp.97-108.

Mabee, B., 2007. Re-imagining the Borders of US Security after 9/11: Securitisation, Risk, and the Creation of the Department of Homeland Security. Globalizations, 4(3), pp.385-397.

Masters, J. (2018). Russia, Trump, and the 2016 U.S. Election. [online] Council on Foreign Relations. Available at: https://www.cfr.org/backgrounder/russia-trump-and-2016-us-election [Accessed 6 Mar. 2019].

Masters, J. (2018). Russia, Trump, and the 2016 U.S. Election. [online] Council on Foreign Relations. Available at: https://www.cfr.org/backgrounder/russia-trump-and-2016-us-election [Accessed 9 April 2019].

McDonald, M., 2008. Securitization and the Construction of Security. *European journal of international relations*, *14*(4), pp.563-587.

Miroff, N. (2018). Hacking, cyberattacks now the biggest threat to U.S., Trump's Homeland Security chief warns. [online] The Washington Post. Available at: https://www.washingtonpost.com/world/national-security/hacking-cyberattacks-now-the-biggest-threat-to-us-trumps-homeland-security-chief-warns/2018/09/05/d0045800-b119-11e8-a20b-5f4f84429666_story.html?noredirect=on&utm_term=.8e72e4975374 [Accessed 9 Apr. 2019].

Monroe, J. (2003). The FBI's Cyber Division. [online] Federal Bureau of Investigation. Available at: https://archives.fbi.gov/archives/news/testimony/the-fbis-cyber-division [Accessed 16 Mar. 2019].

Moodie, J.R. and Holst, C., 2014. For the sake of democracy? The European Commission's justifications for democratising expertise. Expertise and Democracy, pp.293-321.

Moore, A., 2014. Democratic theory and expertise. Between competence and consent. Expertise and Democracy, 1, pp.14-57.

National Infrastructure Advisory Council (NIAC) (2017). Addressing Urgent Cyber Threats to Critical Infrastructure. [online] Available at: https://www.dhs.gov/sites/default/files/publications/niac-securing-cyber-assets-final-report-508.pdf [Accessed 9 Apr. 2019].

National Security Agency (NSA). (n.d.). Cybersecurity. [online] Available at: https://www.nsa.gov/What-We-Do/Cybersecurity/ [Accessed 16 Mar. 2019]. A

National Security Agency (NSA). (n.d.). Signals Intelligence. [online] Available at: https://www.nsa.gov/what-we-do/signals-intelligence/ [Accessed 16 Mar. 2019]. B

Nissenbaum, H., 2005. Where computer security meets national security. *Ethics and Information Technology*, *7*(2), pp.61-73.

O'Connell, M.E., 2012. Cyber security without cyber war. *Journal of Conflict and Security Law*, *17*(2), pp.187-209.

Obama, B. (DHS). (2011). Presidential Policy Directive 8: National Preparedness. [online] Available at: https://www.dhs.gov/presidential-policy-directive-8-national-preparedness [Accessed 5 Mar. 2019].

Obama, B., Executive Order—Improving Critical Infrastructure Cybersecurity.[Online] The White House, February 12, 2013. [online] Available at: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity [Accessed 5 Mar. 2019]

Perrow, C., 2006. Disaster after 9/11 The Department of Homeland Security and the Intelligence Reorganization.

Rodriguez, J. and Jin, B. (2019). The Mueller indictments so far: Lies, trolls and hacks. [online] POLITICO. Available at: https://www.politico.com/interactives/2018/interactive_mueller-indictments-russia-cohen-manafort/ [Accessed 6 Mar. 2019].

Roesner, F., Kohno, T. and Wetherall, D., 2012, April. Detecting and defending against third-party tracking on the web. In Proceedings of the 9th USENIX conference on Networked Systems Design and Implementation (pp. 12-12). USENIX Association. [online] Available at: https://www.usenix.org/system/files/conference/nsdi12/nsdi12-final17.pdf [Accessed 15 Mar. 2019]

Rollins, J. and Henning, A., 2009. Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations. Washington, DC: Congressional Research Service (No. 7-5700, p. R40427). Report. [online] Available at: https://fas.org/sgp/crs/natsec/R40427.pdf [Accessed 5 Mar. 2019]

Rudner, M., 2013. Cyber-threats to critical national infrastructure: An intelligence challenge. *International Journal of Intelligence and CounterIntelligence*, *26*(3), pp.453-481.

Russell, J.A., 2006. Peering into the abyss: Non-state actors and the 2016 proliferation environment. Nonproliferation Review, 13(3), pp.645-657.

Sales, N.A., 2012. Regulating cyber-security. *Nw. UL Rev.*, *107*, p.1503.

Steed, Danny. "The strategic implications of cyber warfare." In Cyber Warfare, p. 81-83. Routledge, 2015

Stohl, M., 2006. Cyber terrorism: a clear and present danger, the sum of all fears, breaking point or patriot games?. *Crime, law and social change*, *46*(4-5), pp.223-238.

Symantec. (2017). What you need to know about the WannaCry Ransomware. [online] Available at: https://www.symantec.com/blogs/threat-intelligence/wannacry-ransomware-attack [Accessed 6 Mar. 2019].

Taureck, R., 2006. Securitization theory and securitization studies. *Journal of International Relations and Development*, *9*(1), pp.53-61.

The Constitution of the United States: A Transcription. (n.d.). [online] Available at: https://www.archives.gov/founding-docs/constitution-transcript [Accessed 11 Apr. 2019].

The White House (2003). The National Strategy to Secure Cyberspace. Washington DC. [online] Available at: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf [Accessed 5 Mar. 2019]

The White House (2013). Presidential Policy Directive -- Critical Infrastructure Security and Resilience. Washington DC. [online] Available at: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil [Accessed 5 Mar. 2019]

The White House (2015). SECURING CYBERSPACE - President Obama Announces New Cybersecurity Legislative Proposal and Other Cybersecurity Efforts. Washington DC. [online] Available at: https://obamawhitehouse.archives.gov/the-press-office/2015/01/13/securing-cyberspace-president-obama-announces-new-cybersecurity-legislat [Accessed 5 Mar. 2019]

The White House (2016). Presidential Policy Directive -- United States Cyber Incident Coordination. Washington DC. [online] Available at: https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident [Accessed 5 Mar. 2019]

The White House (2017). Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. [online] Available at: https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/ [Accessed 9 April 2019]

The White House (2018). National Cyber Strategy of the United States of America. Washington DC. [online] Available at: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf [Accessed 5 Mar. 2019]

The White House (2018). National Cyber Strategy of the United States of America. Washington DC. [online] Available at: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf [Accessed 9 April 2019]

The White House President Barack Obama (2011). International Strategy for Cyberspace. Washington DC. [online] Available at: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf [Accessed 5 Mar. 2019]

The White House President Barrack Obama (The White House) (2011). International Strategy for Cyberspace. [online] Available at: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf [Accessed 9 April 2019]

The White House. (2001). Executive Order 13228. [online] Available at: https://fas.org/irp/offdocs/eo/eo-13228.htm [Accessed 6 February 2019].

Thies, C.G., 2002. A pragmatic guide to qualitative historical analysis in the study of international relations. *International Studies Perspectives*, *3*(4), pp.351-372.

Truman, H. (1950). NSCID 9 COMMUNICATIONS INTELLIGENCE March 10, 1950. [online] Federation of American Scientists. Available at: https://fas.org/irp/offdocs/nscid09.htm [Accessed 16 Mar. 2019].

Trump, D. (DHS) (2017). Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. [online] Available at: https://www.dhs.gov/cisa/executive-order-strengthening-cybersecurity-federal-networks-and-critical-infrastructure [Accessed 6 Mar. 2019].

U.S. Chamber of Commerce. (n.d.). Critical Infrastructure Protection, Information Sharing and Cyber Security. [online] Available at: https://www.uschamber.com/issue-brief/critical-infrastructure-protection-information-sharing-and-cyber-security [Accessed 16 Mar. 2019].

U.S. Cyber Command. (n.d.). Command History. [online] Available at: https://www.cybercom.mil/About/History/ [Accessed 16 Mar. 2019]. A

U.S. Government Accountability Office (GAO) (2017). CYBERSECURITY: DHS's National Integration Center Generally Performs Required Functions but Needs to Evaluate Its Activities More Completely. [online] Available at: https://www.gao.gov/assets/690/682435.pdf [Accessed 5 Mar. 2019]

U.S. Government Accountability Office (GAO) (2018). CYBERSECURITY: DHS Needs to Enhance Efforts to Improve and Promote the Security of Federal and Private-Sector Networks. [online] Available at: https://www.gao.gov/assets/700/691439.pdf [Accessed 5 Mar. 2019]

U.S. Government Publishing Office (2008). COMPILATION OF HOMELAND SECURITY PRESIDENTIAL DIRECTIVES (HSPD) (Updated through December 31, 2007). Washington DC. [online] Available at: https://www.govinfo.gov/content/pkg/CPRT-110HPRT39618/pdf/CPRT-110HPRT39618.pdf [Accessed 5 Mar. 2019]

United States. (2001). The USA PATRIOT Act: preserving life and liberty: uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism. [Washington, D.C.], [U.S. Dept. of Justice]. [online] Available at: http://purl.access.gpo.gov/GPO/LPS39935. [Accessed 5 Mar. 2019]

Van Aelst, P. and Walgrave, S., 2016. Political agenda-setting by the mass media. Ten years of recent research (2005–2015). *Handbook of Public Policy Agenda-setting, Cheltenham: Edgar Elgar*.

Van Dijk, T.A. ed., 2011. *Discourse studies: A multidisciplinary introduction*. Sage.

Van Dijk, T.A., 1997. What is political discourse analysis. *Belgian journal of linguistics*, *11*(1), pp.11-52.

Wæver, O., 1995. *Securitization and desecuritization* (p. 48). Copenhagen: Centre for Peace and Conflict Research.

Walgrave, S. and Van Aelst, P., 2006. The contingency of the mass media's political agenda setting power: Toward a preliminary theory. *Journal of communication*, *56*(1), pp.88-109.

Walgrave, S. and Van Aelst, P., 2006. The contingency of the mass media's political agenda setting power: Toward a preliminary theory. Journal of communication, 56(1), pp.88-109.

Wang, J., 2014. Criticising images: critical discourse analysis of visual semiosis in picture news. *Critical Arts*, *28*(2), pp.264-286.

Weimann, G., 2004. *Cyberterrorism: How real is the threat?* (Vol. 31). United States Institute of Peace.

Weimann, G., 2005. Cyberterrorism: The sum of all fears?. *Studies in Conflict & Terrorism*, *28*(2), pp.129-149.

Weiss, G. and Wodak, R. eds., 2007. Critical discourse analysis. New York, NY: Palgrave Macmillan.

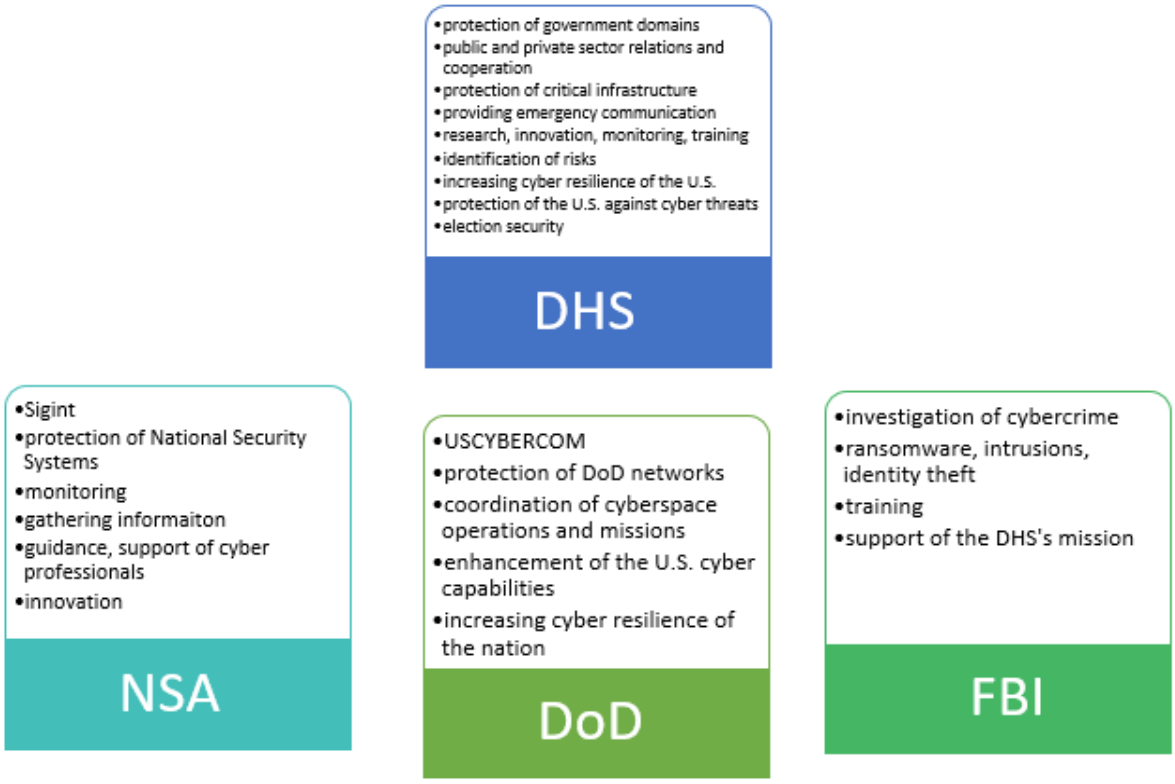
White House, 2009. Cyberspace policy review. *Assuring a Trusted and Resilient Information and Communications Infrastructure." Washington, DC: White House*.

Wirtz, J.J., 2017. The Cyber Pearl Harbor. Intelligence and National Security, 32(6), pp.758-767.

Yourish, K. and Griggs, T. (2018). 8 U.S. Intelligence Groups Blame Russia for Meddling, but Trump Keeps Clouding the Picture. [online] New York Times. Available at: https://www.nytimes.com/interactive/2018/07/16/us/elections/russian-interference-statements-comments.html [Accessed 6 Mar. 2019].

List of Appendices

Appendix no. 1: Main responsibilities and capabilities of federal agencies and departments



Source: Department of Homeland Security (DHS). (n.d.). About CISA. [online] Available at: https://www.dhs.gov/cisa/about-cisa [Accessed 16 Mar. 2019].; Federal Bureau of Investigation (FBI). (n.d.). Addressing Threats to the Nation's Cybersecurity. [online] Available at: https://www.fbi.gov/file-repository/addressing-threats-to-the-nations-cybersecurity-1.pdf/view [Accessed 16 Mar. 2019].; U.S. Cyber Command. (n.d.). Command History. [online] Available at: https://www.cybercom.mil/About/History/ [Accessed 16 Mar. 2019].; Department of Defense (2018). Summary Department of Defense Cyber Strategy. [online] Available at: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF [Accessed 16 Mar. 2019].

Appendix no. 2: Complete list of literature used for the historical analysis and discourse analysis

Administration	Name of Document	Release Date	Main author/sponsor
Reagan	National Policy on Telecommunications and Automated Information Systems Security	9/17/1984	Ronald Reagan

Clinton	Critical Foundations Protecting America's Infrastructures	10/13/1997	President's Commission on Critical Infrastructure Protection
	Joint Doctrine for Information Operations	10/9/1998	Joint Chief of Staff
George W. Bush	Executive Order 13231 of October 16, 2001: Critical Infrastructure Protection in the Information Age	10/16/2001	George W. Bush
	Uniting And Strengthening America by Providing Appropriate Tools Required to Intercept And Obstruct Terrorism (Usa Patriot Act) Act Of 2001	10/26/2001	Congress
	Public Law 107-296: Homeland Security Act of 2002	11/25/2002	Congress
	National Strategy to Secure Cyberspace	2/1/2003	White House Office
	Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization and Protection	12/17/2003	George W. Bush
	Cybersecurity for the Homeland	12/1/2004	Department of Homeland Security
	Creating a National Framework for Cybersecurity: An Analysis of Issues and Options	2/22/2005	Fischer, Eric A.
	Homeland Security Presidential Directive – 16: National Strategy for Aviation Security	3/26/2007	George W. Bush
	National Security Presidential Directive 54/Homeland Security Presidential Directive 23	1/8/2008	George W. Bush
Obama	Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure	5/29/2009	National Security Council, Department of Homeland Security
	Enabling Distributed Security in Cyberspace	3/23/2011	Department of Homeland Security
	Presidential Policy Directive / PPD-8: National Preparedness	3/30/2011	Barack Obama
	International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World	5/1/2011	Barack Obama
	Presidential Policy Directive 20 (PPD-20)	10/1/2012	Barack Obama
	Executive Order 13636: Improving Critical Infrastructure Cybersecurity	2/12/2013	Barack Obama

	Presidential Policy Directive 21: Critical Infrastructure Security and Resilience	2/12/2013	Barack Obama
	Presidential Policy Directive 41: Directive on United States Cyber Incident Coordination	7/26/2016	Barack Obama
Trump	CYBERSECURITY: DHS's National Integration Center Generally Performs Required Functions but Needs to Evaluate Its Activities More Completely	2/1/2017	U.S. Government Accountability Office
	Executive Order 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure	5/11/2017	Donald Trump
	National Infrastructure Advisory Council Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure Final Report	8/1/2017	Department of Homeland Security
	Report to the President on Federal IT Modernization	12/13/2017	Department of Homeland Security, American Technology Council (ATC), Office of Management and Budget (OMB), key government officials
	Homeland Security Information Network 2017 Annual Report	4/1/2018	Department of Homeland Security
	CYBERSECURITY: DHS Needs to Enhance Efforts to Improve and Promote the Security of Federal and Private-Sector Networks.	4/24/2018	U.S. Government Accountability Office
	Federal Cybersecurity Risk Determination Report and Action Plan	5/1/2018	Department of Homeland Security, Office of Management and Budget
	U.S. Department of Homeland Security Cybersecurity Strategy	5/15/2018	Department of Homeland Security
	National Cyber Strategy of the United States of America	9/20/2018	Donald Trump, National Security Council
	Cybersecurity and Infrastructure Security Agency Act of 2018	11/16/2018	Congress

Source: Compiled data from online sources and revelant literature

Appendix no. 3: List of literature used for the discourse analysis in the Atlas.ti

Administration	Name of Document	Release Date	Main author/sponsor
Obama	Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure	5/29/2009	National Security Council, Department of Homeland Security
	Enabling Distributed Security in Cyberspace	3/23/2011	Department of Homeland Security
Trump	National Infrastructure Advisory Council Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure Final Report	8/1/2017	Department of Homeland Security
	Report to the President on Federal IT Modernization	12/13/2017	Department of Homeland Security, American Technology Council (ATC), Office of Management and Budget (OMB), key government officials
	Homeland Security Information Network 2017 Annual Report	4/1/2018	Department of Homeland Security
	Federal Cybersecurity Risk Determination Report and Action Plan	5/1/2018	Department of Homeland Security, Office of Management and Budget
	U.S. Department of Homeland Security Cybersecurity Strategy	5/15/2018	Department of Homeland Security

Source: Compiled data from online sources and relevant literature