Defending Forward: Is the US Cybersecurity Strategy precipitating a security dilemma?

The CyberSecurity Dilemma

Student name: Antonia Gripioti, s2380382

Master Thesis

Program: Crisis and Security Management

January, 2020

Wordcount: 20,620

Contents

1 Introduction

While cybersecurity has been a spreading concern in the United States, incidents such as the Russian interference in the 2016 U.S. presidential election have drawn public and political attention on issues of cyberattacks. Over the last few years, cyberwar has been regularly invoked in the media as well as in the academic and political discourses. Attacks occurring in the cyber realm are rapidly gaining momentum. The Pentagon alone counts millions of cyberattacks towards a variety of targets every day (Fung, 2013). Most are trivial but some of them have proven to be rather disruptive or a significant threat to national security. One clear example of a sophisticated threat was the U.S. – Israeli Stuxnet attack on Iran's nuclear facilities (2010).

To date, Stuxnet is the most sophisticated cyber incident to have been launched. While many take the case of Stuxnet to illustrate the vulnerability of states against advancing cyber technologies, Lindsay (2013) furthers the notion that power demonstrated in the cyber domain is often leveraged by powerful states to enhance their capabilities, much like Russia, China and in our case, the United States. The Stuxnet attack was the turning point in the evaluation of the real threat that cyberspace might constitute. As a result, some observers have begun to question the rhetoric of cyberconflict in the U.S. national security discourse. This rhetoric has framed cybersecurity mainly by utilizing metaphors of war and doom scenarios. This general concern can be summed up in former Defense Secretary Leon Panetta's words that warned about a "cyber Pearl Harbour" (Panetta, 2012). Cyber war skeptics, however, motivated by the Clausewitzian school of war claim that "not one single past cyber offense, neither a minor nor a major one, constitutes an act of war on its own" (Rid, 2011, p.11). The Stuxnet attack and its success thus changed the notion of vulnerability in computer networks and critical infrastructure.

As a consequence, as states witnesses those acts of power and feel threatened, they would reach out and protect themselves, in one way or another. Demchak and Dombrowski (2011) accurately predict an emerging "cybered Westphalian age", where states seek to protect their citizens, their economy and their critical infrastructure. They further observe that already key major powers of the international arena, such as China and the Unites States, are demonstrating a cybered territorial sovereignty posture, with other nations expected to follow. The ever-rising perception of an imminent cyberattack deems the state as ready to defend against, repel, or

prevent whatever could threaten its cyber sovereignty and willing to do so with military resources if required (Ibid.)

1.1 researching cybersecurity in the context of international relations

"The environment we operate in today is truly one of great-power competition, and in these competitions, the locus of the struggle for power has shifted towards cyberspace" Paul Nakasone, head of the National Security Agency, mentioned in a speech at the Billington Cybersecurity Summit. The importance of cyber security as an emerging issue in the realm of international relations cannot be overstated.

Originating with Arquila and Ronfeldt's (1993) concept of netwar and cyber war, an extensive history of theoretical and political examinations on cyberspace has inscribed on the international community. For realists, advanced military capabilities are key to deterring aggressors and maintaining national security (Morgenthau, 1948). In this regard, the US Department of Defense (DoD) defines deterrence as the 'prevention from action by fear of the consequences'. Deterrence is a state of mind brought about by the existence of a credible threat of unacceptable counteraction (DoD, 1997). More accurately, Paul Huth defines deterrence as *"the use of threats by one party to convince another party to refrain from initiating some course of action"* (Huth, 1999). Thus, the main focus of the strategic deterrence theory, which rose to prominence during the Cold War, was the threat of mutually assured destruction from nuclear weapons.

Relying on deterrence theory, Morgan, Philbin, Nye and Bendiek and Metzger propose the application of nuclear era approaches, based on mutually assured destruction (MAD), to the cyber domain (Morgan, 2010; Philbin, 2013; Nye, 2011; Bendiek and Metzger, 2015). Lonsdale later introduces the warfighting approach in the cyber realm. In nuclear deterrence nuclear weapons were considered part of a much more complicated strategy that ensured deterrence (Lonsdale, 2018).

The mutual assured destruction concept emerged through the Cold War era of nuclear weapons, when both conflicted sides developed a significant nuclear offensive capability enough to obliterate the other side (Swift, 2009). More specifically, there were certain systems and procedures developed that could detect launches from the other side and then allow a counter response. As a result, there was no first strike advantage as instant retaliation would follow and

equal decimation was bound to occur. In this context, each side perceived the other to be a "sensible rational opponent" deterred by the "threats of nuclear retaliation" from the other party (Curtis, 2000). The incentive for a first strike was mutually annulled because victory was not guaranteed and both parties were unwilling to take any action that could ultimately lead to their own annihilation. In this interpretation, one might argue that this behavior of two conflicted sides could be observed also in the digital commons. That is, a state attempting to demonstrate its power in cyberspace could cause insecurity to other states, thus provoking them to respond accordingly. How would that affect the balance in the international system? What if the Unites States are already demonstrating a change in their behavior within the cyber domain?

In September 2018, President Trump signed the National Cyber Strategy, the first fully articulated cyber strategy since 2003 (White House, 2018). The new document entails several important changes in the direction of cyber-response. This new Strategy essentially replaces restrictions on the use of a more offensive posture in cyberspace with a new legal regime that enables the US Defense Department to operate with greater authority. National Security Advisor, John Bolton, describes this new strategy as an endeavor to "create powerful deterrence structures that persuade the adversary not to strike in the first place" (Groll, 2018).

The Department of Defense, in its newly released strategy document in 2018, further announced that they would "defend forward" US networks and infrastructure by disrupting *"malicious cyber activity at its source" and endeavor to "ensure there are consequences for irresponsible cyber behavior" by "preserving peace through strength"* (White House, 2018). In addition to this, great-power strategic competition and preparation for war are the other central tenets of the new strategy. Its content renders it more focused, risk-acceptant and confidently more active than its predecessor in 2015 (DoD, 2015). All the aforementioned are new terms included in the strategy that call for further explanation, such as "defending forward", "persistence", and "defense critical infrastructure". Overall, it seems like the US cyber defense strategy has moved past traditional deterrence strategies and welcomes the possibility to confront enemies before approaching.

This shift from reactive to preemptive action in the cyber domain not only marks the departure from the 2015 US cyber strategy, but also responds to the persistent cyber campaigns targeting the US infrastructure. Looking at these incidents individually, they may fall sort of

provoking an official cyber response, but their cumulative impact cannot be overlooked. Kollars and Scheider argued that this new forward-leaning stance of the United States seeks to address the upcoming threats without risking an escalation to further use of force (2018), whereas others might consider it a rather provocative stance.

This paper relies on this realistic and imminent concern. The chosen theoretical basis frames the analysis that follows based on the new policy paper that the DoD issued in 2018. Doing so, it provides a window into the evolving nature of cybersecurity in the United States' threat perceptions, seemingly confirming the DoD's classification of cyberspace as a "domain of war" (Pellerin, 2010). Although the details of the new strategy are classified, the unclassified issued summary has attracted a lot of attention in the political and academic discourses. "The 2018 DoD cyber strategy prioritizes the challenge of great power competition and recognizes that the department must adapt a proactive posture to compete with and counter determined and rapidly maturing adversaries," said Kenneth Rapuano, the assistant secretary of Defense for homeland defense and global security. It makes clear that DoD's focus on cyberspace, like in other domains, is to prevent or mitigate threats before they reach American soil. The central idea of the strategy is focused on the US military's duty to 'defend forward' to ensure the integrity of US networks. It is an original approach supported by the Trump administration, who is eager to loosen most of the restrictions applied on military cyber operations during Obama's administration. As the DoD increasingly fears of damage caused by cyberattacks, national security leaders and security scholars are debating the best preventive strategy. The main challenge lays on the dilemma of whether to adopt a strategy that could halt an attack or to try and dissuade adversaries from acting on their attack.

> *"When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. We reserve the right to use all necessary means — diplomatic, informational, military, and economic — as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests. In so doing, we will exhaust all options before military force whenever we can; will carefully weigh the costs and risks of action against the costs of inaction; and will act in a way that reflects our values and strengthens our legitimacy, seeking broad international support whenever possible."*

—International Strategy for Cyberspace, The White House, 2011

The United States maintain a history of providing new models for national-level security initiatives, especially related to military organizations (Goldman and Eliason, 2013). In this case, announcing a new cybersecurity strategy, with not enough official details, provokes a new debate in the international politics and security. In the fall of 2010, the US Cyber Command became operational as a response to the rising probability of a cyber conflict. Following that, we have already witnessed states associated with the United States either mirroring or desiring the same functions for their nation-state. For instance, South Korea also employs a military cyber command and the United Kingdom has gradually been considering a close integration of military and intelligence cyber resources (Louis, 2011). To this day, the United States have declared cyber threats as major national security concerns, created a new major military unit, and managed to not only justify, but also fortify their national ability to forestall cyber attacks (Demchak and Dombrowski, 2011). However, the recent policy changes in the Trump administration could amplify the escalation or hamper the effectiveness of any attempt to ensure security and survival in cyberspace.

1.2 research question and relevance

The purpose of this thesis is to answer the following question:

- To what extent is the US Cybersecurity Strategy precipitating a security dilemma and how has the US government legitimized its strategy since 2015?

The question of whether strategic deterrence in cyberspace is applicable is a topic of contention among scholars and policy-makers. However, this paper aims to examine the traditional strategic deterrence theory and its relevance with deterrence in the fifth battlespace domain, namely cyberspace. In this attempt, the conceptual basis of deterrence theory will be reviewed, alongside with a brief mention to nuclear weapons, as well as international relations theories. The thesis will follow up on this main question with the subsequent sub-questions: *Could offensive capabilities be effective in deterring attacks in cyberspace? Under what circumstances could increasingly sophisticated cyber operations lead to escalation or further military violence and insecurity among states?*

The argument presented explains that the behavior of a great, military and economic power such as the United States certainly affects the behavior of the actors in the global system.

The paper does not attempt to investigate to what extend deterrence theory applies to cyberspace. It rather focuses on the ramifications of an offensive deterrence national strategy. A potential cyber-deterrence strategy that introduces - for the first time in any legal or official policy document - the term “defend forward” might enhance national security against devastating cyberattacks, but it could simultaneously cause instability and insecurity to the rest of the international community. To an extent, Kello’s (2013) assumption is appreciated, which suggests that the future of cyber war will forever change the way states interact with each other.

1.3 Methodology

The scope of this research is limited to a theoretical exploration of the United States adopting a more offensive cyber strategy. Further, the US adopting the nuclear mutually assured destruction strategy of the 1960s kickstarts this thesis and is used as a historical parallel study in order to examine the theoretical prospect of this strategy. Firstly, a few points need to be addressed, such as the purpose of this research, which is not to determine whether deterrence is effective as a cyber security strategy. The literature around cyber security strategies might be scarce, yet numerous authors have attempted to examine this issue in depth and their conclusions diverse (Morgan, 2003; Philbin, 2013; Nye, 2011). Since this thesis does not aim to answer the question of whether deterrence theory is applicable in cyberspace, two assumptions are made; first, deterrence, if properly implemented, is effective in the cyber realm; second, the US nuclear strategy was effective at deterring the escalation of the conflict during the Cold War.

Second, there are numerous potential cyber threats and the first attempt at classifying them divides them into state and non-state actors. However, it is clear that a common strategy is not necessarily the most optimum one as well as a strategy that deters one enemy, might not deter the other. For instance, the US nuclear deterrent strategy, when originally developed, was aimed at state actors, and more specifically the Soviet Union. This thesis is limited to examining the theoretical framework of deterrence strategy aiming at other nation states. There is no intention to address the issue of deterring offensive behavior on cyber space initiated by hackers, terrorists or even other organized criminal associations.

To support this thesis’ main argument, I will focus on the US cybersecurity policy developments during the last two presidencies, the Obama administration (2009-2017) and the Trump administration (2017-present). During the summer of 20018 the Trump administration

faced a series of stark choices for cyber operations against American adversaries (Data breaches and exposures, hackers targeting US Universities, etc.). Following the efforts of 2017, granting more leeway to military officials and commanders to make instant decisions on the field the President signed an order (August 15) delegating authority to the defense secretary to use cyber tools and techniques to support their operations in cyberspace, loosening rules established under the previous administration. This paper goes beyond the identification and taxonomy of cyber threats and draws attention to their incorporation in national security strategies. This paper aims to explain the relationship between political discourse and military practices.

A national cybersecurity strategy is considered to be a plan of actions to improve security and resilience. Besides establishing national objectives and priorities, such an official governmentally issued paper builds a strategy. The concern raised in this paper regarding the power shifts in the international system will be explored by relying on Antonio Reyes's framework to analyze legitimization in political discourse. In the effort to understand the US cybersecurity doctrine, it is essential to acknowledge two highly important debates in political science. Firstly, the debate over the offense-defense balance in the international system struggling to explain the underlying logic of the 'security dilemma'. Secondly the debate over deterrence seeking to comprehend the ways in which Cold War adversaries could reach a mutual understanding against nuclear weapons and its deployment.

I will rely on international relations theories and more specifically on the concepts of deterrence in a newly established warfighting domain, cyberspace, in correlation to the weapons of mass destruction during the Cold War. Other basic concepts auxiliary for my analysis revolve around the balance of power in the international community, states' desire to shift or maintain the status quo and the precipitation of the security dilemma.

The aforementioned discursive analysis will be complemented by a contextual acknowledgement of the political environment in which each policy paper was published. The United States have substantial capabilities in both defense and power projection in cyberspace which have developed in response to growing and more complicated threats. The increase of possible sophisticated threats in the cyber realm have affected the US' foreign policy and the following paper is called for identifying which strategies are prioritized or excluded and how this new development will create its own chain of events in the international arena.

All in all, the implications of aggressive cyber activity for international order, or anarchy, have yet to be explored. Security scholars have paid little attention to applying their theoretical frameworks to explain or predict competition in the cyber domain (Kello, 2013). As a result, the conceptual apparatus of international security, and more specifically cybersecurity, is still immature. Political authorities have only recently started to include cyberspace in their strategy discourse and it is intriguing to investigate how they chose to justify and legitimize state behavior. For this reason, the academic relevance of this paper will permit the utility of Reyes's (2011) interdisciplinary framework of analysis on the process of legitimization through the use of language and, following, the nexus between national deterrence strategies in cyberspace and their impact in the international arena. Answering the aforementioned issues will allow the onset of an academic discourse regarding security in cyberspace and the path that individual states have started on their own towards controlling the way the world wide web affects their sovereignty, their citizens, infrastructure and other critical elements of the society.

This thesis relies on the following basis. As the Internet spread designed on the principle to facilitate information sharing and ease of use instead of facilitating a militarized environment, an offensive strategy within the cyber domain has an advantage over a defensive one. More specifically, in the other domains where the governments have the monopoly for use of force, i.e. the military, resources are costly, the defender protects their territory till attrition or exhaustion. On the contrary, a governmental offense in the virtual world has little costs, the actors involved are diverse and anonymous. This renders the effective use of counterforce strategies rather narrow. In that sense, a potential threatening cyber activity, although only incipient, is still imminent. A massive disruption could have implications on a state's sovereignty, infrastructure or civilians. Despite the fact that technology keeps evolving, typical responses to cyberattacks include offensive capabilities and deterrence strategies, and are not limited to ensuring network and infrastructure resilience (Bandiek and Metzger, 2015). This development in cybersecurity policy illustrates the core questions around deploying offensive cyber operations. Great power competition in the 21st century has been exploiting the high correlation of our contemporary world online with the aim to undermine rivals. This topic has attracted major debates within the political arena with questions such as the possibility for offensive cyber operations to accomplish state foreign policy objectives; or under what circumstances increasingly sophisticated cyber operations could lead to escalation or further military violence and insecurity among states. In

that sense, the hypothesis of this thesis is that such a strategy that implies and justifies an offensive deterrent strategy can credibly precipitate the security dilemma of nation-state actors and could potentially lead to 'new Cold War'.

1.4 Reading Guide

Following this introduction, Chapter Two presents a background of the academic literature on cybersecurity and provides with key definitions regarding this domain. Chapter Three lays the theoretical groundwork for the empirical analysis. The realist paradigm of international relations theories is explained, including some basic notions around the military strategy of deterrence. Chapter Four explains the methodology used for the analysis, detailing the case selection and laying out the conceptual framework utilized as the backbone of the analysis. The following chapters constitute the main body of the analysis of Obama's and Trump's aspirations regarding their national cybersecurity policies. Lastly, the final chapter summarizes the main findings of this thesis and identifies both limitations and opportunities for further research.

2 Literature Review

Given the complexity and inadvertence of the phenomenon at hand, the following review introduced the key definitions of technical terms associated with cyberspace and cybersecurity. The cyber domain is a relatively under-researched notion and its everchanging character adds more challenges to its understanding. As this thesis discusses war within cyberspace, it is essential to distinguish between the differing activities occurring within such a realm, from cyber espionage to cyber terrorism. In order to proceed with the analysis of this thesis, it is important to clarify the meaning behind the notions and to understand some common technical aspects. The study of international security requires commonly accepted technical concepts that explain the various dimension of the cyber realm. First and foremost, defining complex cyber properties allows for a deeper understanding, followed by better identification of related phenomena to national and international security. For the purpose of this study, the following schematization is adopted.

As a starting point, author William Gibson in his early 1980's novel envisioned the term cyberspace as "the network of computers through which the characters in his futuristic novels travel" (Krebs, 2005). On another note, the National Strategy to Secure Cyberspace mentions that "Cyberspace is their nervous system—the control system of our country (Office of the President of the US, 2003). The U.S. Defense Department describes *cyberspace* as a new "war fighting domain" alongside the physical land, sea, air, and space domains (Lynn III, 2010). DOD's definition for cyberspace is "A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers"(DoD, 2011).

The cyber domain, compared to the other geostrategic domains, lacks a historical perspective and further scrutiny. In this context, Nye's definition of cyberspace is useful for political analysis. The cyber realm consists of the Internet, the network of connected computers around the world, and also of the infrastructure that sustains this network of networks, such as intranets, fiber-optic cables and so on. This physical layer of cyberspace abides by not only the political laws of sovereign jurisdiction but also by the economic laws of the global market. However, most issues occur at the informational layer of this cyber-construction. When attacks

targeted at the informational realm are spilled over the physical realm, the cost is high and the resources are scarce (Nye, 2011, p.19). As disturbances might have both territorial and extraterritorial consequences, control is mandatory towards any cyber activity within or outside the domain of cyberspace. Jason Healey predicts that "a cyberattack will destroy not only ones and zeros, but things made of steel and concrete" (Healey, 2014). Basically, cyberspace establishes the technical markers within which virtual activities operate (Kello, 2013).

The term *cyber power* highlights the political relevance of modern technologies. Since politics refers to the distribution of influence, then cyber power is another expression of attempts to control access and activity in the aforementioned domain. Valeriano and Maness (2015, p.28) define cyber power as the ability to apply typical forms of control and domination in cyberspace. When it comes to control over cyberspace it is much more complicated than in other domains. Governments cannot control their cyber-borders and the states sovereignty online the same way they can defend their borders on land, sea, air or space. The multi-layered Internet became one of the most powerful contemporary instruments that is lacking governmental regulations (European Commission, High Representative of the Union 2013, p. 3). On the contrary, the barriers to enter the cyber domain are low and even great powers are highly unlikely to establish dominance. In line with this, it makes little sense to argue about dominance in cyberspace. While having greater resources, the largest powers, such as the United States, Russia, China etc., also have great vulnerabilities (i.e. sharing intelligence with allies, interconnectedness of networks, etc.).

Around the domain of cyberspace other key actions orbit and demand some clarification, especially when policy and government setting are in place. More specifically, the term *cyberattack* is commonly used as an umbrella term that covers a wide range of actions from simple denial of service to espionage. A cyberattack refers to the use of code to interfere with or disturb a computer network for the purpose of a political or strategic agenda (Ibid). If the implications of a cyberattack cause serious physical destruction or even casualties, then this action could be labeled as cyberwar. (Finlay, 2018). The term *cyber war* is used even more vaguely by some while others refer to it as "bloodless war", a conflict between states that is confined within the informational or visual layer of cyberspace (Smeets, 2018). Cyberwar was initially associated with military action (Cavelty, 2013). The outcome of a military conflict is based on, first, securing one's own military information, and second, the ability to attack an enemy's military information systems (Isnarti, 2016). In spite of the very nature of cyberspace,

an attack in cyberspace can exceed beyond physical military strategy, as it can affect entire computer systems and disturb a state's digital infrastructure, including but not limited to, transportation, telecommunications, or even nuclear power controls. Nevertheless, a more useful definition for the purpose of this paper is one that does not disregard the interconnection of cyberspace; "hostile actions in cyberspace that have consequences that amplify or are equivalent to major kinetic violence" (Nye Jr., 2011, p.21). For this reason, I use the term *cyber conflict* to describe any cyber malice as interpreted within the international relations context. Cyber conflict is "the use of computational technologies for malevolent and destructive purposes to impact, change, or modify diplomatic or military interactions" (Valeriano and Maness, 2015, p. 21). Having established the definition of key terms that constitute the backbone of any research referring to cyberspace, the next chapter outlines the theoretical framework of this thesis.

3 In theory

The theoretical chapter reviews some relevant literature to the current study. There are different theoretical and analytical tools available for investigating the incorporation of cyberspace in national security policies. I have chosen to utilize deterrence theory within the context of the most dominant international relations theory, realism – and more specifically neorealism, as the main theoretical framework, as it has the ability to stress the competitive and conflictual side of international politics.

3.1 Cyberspace and International Relations Theories

Albeit the fact that the academic research and literature on cyberspace and its elements are scarce, the phenomena occurring in this domain are indeed a matter of International Relations' field mainly because foundational concepts such as sovereignty, anarchy, power, and system are still valid in the discourse of cybersecurity (Cavelty, 2010). To my assessment, International Relations theories provide a conceptual framework upon which the elements of cyberspace can be adequately analyzed. Shifting the focus away from the balance of power system towards a system of collective security, these theories can be utilized as a new lens through which thinkers can glance at the cyberspace and its relevance to the different moves made in the international chess board. After its first emergence as a discipline in academics and further in politics, international relations theories have attempted to discuss war and (inter)national security. As these theories seek to interpret the international arena, realism provides a state centric approach and evolves around the main concern of security. Liberalism asserts cooperation in the international system and regards other actors apart from the state. Taking state and non-state actors' cooperation further, constructivism interprets international phenomena as socially constructed. In that sense, while the latter can better explain why cyber-offences occur, how different actors are involved and liberal traditions can shed a light on how to better solve these new aggressions, this paper utilizes realism in order to interpret state behavior in the conduct of cyber war. The emerging cyber challenges exhibit a resurgence of the realist paradigm with a focus on security, competition, the distribution of power and the benefits of deterrence strategies. As Reardon and Choucri write: "realist theories of deterrence, crisis management, and conflict may be used to understand whether cyberspace is stabilising or destabilising, whether cyber

technologies will be a new source of conflict or of peace, and whether states will engage in cyber arms racing" (2012, p.6).

3.2 Neorealism

Realism encompasses a plethora of approaches claiming a long theoretical tradition in national and international politics, stressing its competitive side. It is a conflict-based paradigm in international relations, in which the key actors are states. The realist tradition traces back to Thucydides' analysis of the Peloponnesian war in the 5th century B.C. where he pinpointed the importance of power in political survival. (Vasquez, 1995). This section of the theoretical chapter examines the neorealist approach in international relations, which argues that states' ultimate goal is maintaining their power and thus continuously compete among themselves, either to gain power or to ensure that they do not lose any. For structural realists, power is the currency of international politics (Mearsheimer, 2001). This competition for power leaves them little choice if they want to survive in this system, under anarchy (Herz, 1950). Under the same light, the more a state feels vulnerable the higher the chances are for it either to join a more secure coalition or to wish to increase its arms capabilities, even to initiate an attack rather than be attacked. On the contrary, if states grow more resilient, they could afford a more relaxed view of threats (Jervis, 1978).

In the 1970s, Kenneth Waltz attempted to cure the defects of classical realism with his more scientific approach, known as neorealism or structural realism. According to Waltz (1979), the uniform behavior of states throughout history can be explained by the trends the structure of the international system imposes. Realists, and especially today's neorealists, deem the absence of a higher authority as a primary determinant of international political outcomes. Although, structural realism is first and foremost a paradigm about outcomes of international interaction, it can also estimate expected state behavior. The international arena essentially relies on a self-help notion, where each state is responsible for its own survival. "Internationally, the environment of states' actions, or the structure of their system, is set by the fact that some states prefer survival over other ends obtainable in the short run and act with relative efficiency to achieve that end" (Waltz, 1979, p.93).

3.2.1. Power and Anarchy

The most basic principle of realism is reflected on the answer to the simple question: why do states want power? Great powers carefully measure their economic and military power in relation to each other, creating the context of power politics. For structural realists, it is the architecture of the international system and the relations among the main actors that force states to seek power. The lack of an international authority creates a system, a chessboard, where the relations between actors are based on anarchy. This means that international anarchy allows for adjustments in the system but at the same time triggers an environment of uncertainty, especially under the absence of international institutions or international law enforcement. In this light, Robert Gilpin argues, "as the power of a state increases, it seeks to extend its territorial control, its political influence, and/or its domination of the international economy" (1981, p.106). As realists envision states in an anarchic system, they likewise consider security in a similar dynamic. In order to ensure their security, states aim to increase their power and to be capable of deterring potential aggressors. In the words of Thucydides in his book *History,* the growth of the Athenian power caused insecurity to the Peloponnesian League and thus propelled them into war (1.23).

Any interaction within this anarchist international system ultimately encourages behavior that might lead the concerned parties to question or challenge the status quo. In the context of anarchy, each state is uncertain about others' intentions and simultaneously is worried about the shift on balance of power. According to John Mearsheimer, "Uncertainty about the intentions of other states is unavoidable, which means that states can never be sure that other states do not have offensive intentions to go along with their offensive capabilities" (2001).

3.3 Offensive and Defensive Realism

Within neorealism, there is a distinction between offensive and defensive realism. On the one hand, offensive realism seeks to increase power and influence in order to achieve security through hegemony. The rationale is illustrated best by John Mearsheimer who notes that "states quickly understand that the best way to ensure their survival is to be the most powerful state in the system (2001, p.33). More specifically, states are never certain how to interpret other states' intentions and as a result all the great powers ultimately increase their power, leading to high levels of competition. On the other hand, defensive realism attributes states' pursue towards moderate and restrained behavior to the anarchic international system. The rationale is that

aggression and competition prove to be unproductive as they will provoke counterbalancing behavior. As Christopher Layne notes, "states balance against hegemons" (1993: 45). Both concepts agree on survival being the state's primary goal, but for defensive realists most states are in favor of the balance of power in the system and thus, seek to maintain the status quo (Waltz, 1979). Nevertheless, offensive realists believe that since the context remains the anarchic international system, then systemic shifts are to occur given that states seek to maximize their power. The neorealist offence-defense balance concept can be utilized to explain state behavior in response to cyber aggression. In addition, according to Robert Jervis this spiral of mutual distrust is more likely to occur when offense prevails over defense. That is when "it is easier to destroy the other's army and take his territory than it is to defend one's own." (Jervis, 1978). Whereas when defense domineers offense, then "is easier to protect and to hold than it is to move forward, destroy, and take," and thus easier for states to protect themselves through defensive rather than offensive measures (ibid). Following Jervis's assumptions, there is least risk of unnecessary war when defense prevails over offense. Conversely, suspicions will be highest where offense and defense are hard to distinguish. Dunne illustrates that:

> "Offence defense balance indicates how easy or difficult it is to conquer territory or defeat a defender in battle. If the balance favours the defender, conquest is difficult and war is therefore unlikely. The reserve is the case if the balance favours the offence" (2013, p.355).

For classical realists, power is an end in itself but for structural realists, power is a means to an end and the utter end is survival (Mearsheimer, 2001). As Fareed Zakaria emphasizes states seek to maximize influence, not power. However, for neorealists, material power remains the most effective instrument of influence and opportunity. Consequently, it is hard to ignore that the way a threat -or an intention- is perceived might affect states' behavior more than objective power. In this context, neorealism can account for the ultimate motives of states, i.e. their basic drive to attain their security and, as a following step, some relative power in order to stand in front of other states' motives.

In addition to the anarchic character of the international system follows the assumption that states possess some offensive military capability in order to be able to protect their territory and interests in case of an attack. This leads to another assumption which claims that states can

never be certain about the intentions of the other actors within the system. The problem here lies with the difficulty to discern another state's intentions. But, undoubtedly, each state's main goal is survival. However, certain circumstances arise where states not only become preoccupied with power and the status quo, but also seek to gain power at each other's expense. As Mearsheimer dully notes, great powers fear each other. They understand that they have to rely on themselves to ensure their survival. In that sense, their greatest fear is that another state might have the capability as well as the motive to threaten them (2001). Knowing this, states realize quickly that the answer is to be especially powerful. The more powerful a state is, the less likely it is that it will be attacked by its competitors. This simple logic frames the main argument of this paper as I try to explain how United States' efforts to strengthen their cyber capabilities could affect the international status quo and could steer competition and imbalance of power. All in all, the aforementioned structural imperatives of the international system according to realists are reflected in the notion of the security dilemma, which will be further elaborated on.

3.4 The Cybersecurity dilemma

Defining the security dilemma in international relations, it all comes down to the basic principle that although all actors aim at a common goal, they cannot be sure that each one will cooperate in order to reach it. The term was introduced by John H. Herz, a German scholar in his book *Political Realism and Political Idealism* (1951). The security dilemma refers to a situation in which a state's intention is to heighten its security. In an anarchic international system, maximum security is achieved either by increasing military capabilities or by making alliances. In a zero-sum world, those developments, though, are not unnoticed by the rest of the actors in the system, and can lead to other states responding with similar measures, irritating the already tense relations and sustaining probable conflict (Jervis, 1978).

Despite the simplicity of looking towards a common goal, some basic difficulties may occur. For instance, no matter how much authorities or policy makers are dedicated to the status quo, fear and uncertainty remain the two important factors leading to changed values and new opportunities, but also new dangers. In addition, the lack of an international authority fosters uncertainty to the not self-sufficient countries who will struggle inadequately to maintain control on their resources and borders. As it has already been observed in international politics, one state's gain inadvertently endangers others, meaning that the means by which a state increases its security might decrease the security of others (Jervis, 1978, p.169).

As mentioned above, the dilemma caused by the ambiguous symbolism of a state raising its military capabilities has strained those responsible for the security of this political community. Mainly, because, they are to decide whether military developments are for defensive purposes, that is to enhance their security, or for offensive purposes, with the aim to tilt the scale to their advantage. Consequently, the same dilemma is reflected on a state's efforts to enhance its capabilities in each war domain, let alone cyberspace.

Conceptually, this behavior in foreign policies is not as advanced as one might think. More specifically, Ben Buchanan in his book The Cybersecurity Dilemma mentions several cases where the National Security Agency (NSA) undertook activities which could easily facilitate the concept of defending forward (Chapter 2). In one specific instance that involved an operation against Chinese networks, where the NSA hacked into their systems and by doing so they developed an excellent map of the cyber-terrain and used the intelligence gather to their advantage. Hence, it is reasonable to assume that the concept of defending forward could give the military the necessary authority to conduct similar -hacking- operations with the utter goal of intelligence gathering and infrastructure manipulation.

Following this assumption, the study of escalation in cyber operations is still in its preliminary stages and one might argue that fits under the broad heading of the classic security dilemma. More specifically, as Buchanan highlights it is difficult for a state under attack to distinguish whether its potential adversaries are preparing the grounds for a cyberattack or whether they are collecting intelligence (2017). It is reasonable to expect that, since it is already difficult for states to discern simple intelligence operations from imminent attacks, then it is even more challenging to distinguish between defending and attacking forward. If the new DoD strategy permits US operations to be more aggressive than before, that could cause significant ramifications in escalation (Ibid).

3.5 Deterrence: then and now.

Albeit being a very valuable concept for achieving restraint, deterrence theory is rather limited towards military security, and more specifically the nuclear, in the postwar era. For this reason, this paper will discuss the extent to which deterrence theory is applicable to cyberspace. Although deterrence does not require nuclear weapons, their existence facilitate the apprehension of its basic ideas (Jervis, 1979). In the case that weapons are not used for defense, it's inevitable

not to raise suspicions on their alternative uses (Quester, 2019). Following the analysis, I will consider the applicability of nuclear deterrence in preventing non-nuclear attacks in the cyber domain in the post-Cold War era with all the technological innovations this period has introduced. The main hypothesis of this section is that the traditional approach of deterrence for nuclear strategy is still relevant in the security dilemma's landscape, and more specifically in the cyber domain.

Analysts are still not confident about the lessons learned from offense, defense, deterrence, and escalation. After reviewing the issue of cybersecurity, I will indicate several lessons learned from the nuclear experience during the Cold War. The two technologies, nuclear weapons and cyberspace, might be vastly distinct yet there are a few observations and comparisons one can make of the ways governments have learned to interact with these technological innovations.

Deterrence theory was the popular framework utilized to explain the influence of nuclear weapons during the Cold War. The main assertion is that the nuclear-armed states would not go to war for fear of the grave consequences a nuclear war would entail. Some authors, recognizing that both domains share some common characteristics, have applied this framework of cyberdeterrence. For instance, in its national cyber security strategy, the US government aims at "convincing a potential adversary that it will suffer unacceptable costs if it conducts an attack on the United States" (Department of Defense, 2015). The term deterrence is defined as "to discourage and turn aside or restrain by fear".[1] A first interpretation grasps two concepts of deterrence, (i) when somebody is discouraged by the opponent's defenses and (ii) restraint for fear of retaliation (Bendiek and Metzger, 2015). In any case, deterrence seeks to maintain the status quo and is reserved in forestalling an attack.

In a way, we deem cyberattacks as an utterly new challenge. However, there are some underlying characteristics that tie them together with nuclear technology. Nuclear weapons, successfully cited as "weapons of mass destruction", are being faced with deterrence strategies and restraint by the avoidance of escalation. Nuclear-states rely on their enemy's second-strike capability and through the manipulation of risk ensure the eluding of actual firing. War in the

[1] Search for word "to deter", Oxford English Dictionary 2014

digital realm could, in theory at least, lead to disturbing or even crippling enemy assets, without costs or any kinetic attacks (Pool, 2013). This section compares operational and strategic characteristics of the two, which describe the nature of the capability and the nature of interaction within politics.

3.6 Cyber-weapons and Cyber deterrence

First and foremost, both nuclear and cyber weapons have posed as disputable issues in international relations. At the same time, cyberattacks offer an opportunity for potential enemies to challenge one of the great powers and overcome their undoubted advantage in conventional military capabilities. What is more, the very nature of cyberattacks, being more instantaneous and difficult for attribution, adds to their advantage. Their ramifications might not end up in countless casualties such as a nuclear attack would generate, but by constant and systematic offenses, they could still paralyze US capabilities and hurt its society and economy (Lynn III, 2010). Such an example, that didn't cause immediate casualties but caused a lot of disruptions was the Stuxnet attack, a 'virus' that mutated and spread enough so as to cause crippling consequences to critical infrastructure.

On the surface, the analogy is indeed compelling. In 2013, Secretary of State John Kerry was reported with the response "I guess I would call it the 21st century nuclear weapons equivalent"(2013). Later that year, Russian Deputy Prime Minister Dmitry Rogozin praised cyberweapons for their first strike capability. This very analogy has allowed many officials to use it as a foundational argument in their advancing military and strategic discourse. In general, I think there are indeed some similarities in their historical evolution. That is, cyber has in many ways replaced the role nuclear demonstrated in world politics a few decades ago. On the surface, the analogy of the two weapons is compelling. Cyber, like nuclear, is not only a weapon, but a leading means through which international relations unfold these days. One undeniable similarity is their effect. Much like nuclear weapons, cyber weapons -especially the most powerful ones, such as malware which targets critical infrastructure and threatens its integrity- can be proven catastrophically destructive and are nearly impossible to defend against. Furthermore, the same way a nuclear warhead can be launched and activated in almost no-time, cyber attacks have short delivery times across vast distances, a characteristic which allows them great momentum and high damage occurrence.

Another dimension to this comparison between cyber and nuclear is that they are both considered as a dual-use technology, military and civilian application. Cyber has proven to be a tool of multiple effects, let alone an instrument of criminal activity. In addition, the illusion of a newly created exclusive cyber club has originated due to the advantage of only a few technologically competent states. The aforementioned tempting similarities and the exponentially threatening nature of cyber attacks has allowed leaders to refer to nuclear deterrence strategies in cyberspace with fair justification (Cirenza, 2016) .

Allowing this comparison to dive a little dipper, the two technologies are far distant from one another. The total destructiveness of nuclear technology is unequivocal, while cyber operations do not pose a clear existential threat. The National Research Council highlights differences in action. Nuclear explosions are indisputable, while some cyber intrusions might go unnoticed for long periods of time or even completely untraceable (Owens et. al., 2009). Furthermore, one might notice an overlap of civilian and nuclear technology whereas the internet has endowed the civilian sector. Its fusion with intelligence operations, military and civilian functions allows cyber to assume a more central role. Finally, while the sheer destructiveness of nuclear attacks is a serious concern, non-state actors gaining access to nuclear materials remain scarce. Despite these differences, Owens et al. (2009) made some observations on the similarities of the two strategies. These include the concept of superiority of offense over defense, the use of weapons for tactical and strategic purposes, and the likelihood of unintended consequences and escalations -especially with a new technology.

The preceding discussion does acknowledge that comparison between the two domains from the aspect of technology is valid. Moving forward, I will outline some important distinctions between cyber war, nuclear weapons and deterrence. First of all, in cyber war the source of the attack might remain ambiguous, in contrast to almost certain identification of a state, even a non-state actor, in case of a nuclear launch. Furthermore, cyberattacks can remain undetected for great periods of time, without causing any obvious disruption, while any use of a nuclear weapon since 1945 by a state would stir the water in the international community, no matter the extent of the explosion. Second, as mentioned before, there haven’t been cyberattacks with severe consequences so far, even the most sophisticated attacks are highly unlikely to cause the enormous damage and casualties just one nuclear head could. The damage caused by an

attack in the cyber realm mostly affects the networks, the information systems and their content. Still, these disturbances could have spillover effects on any economic, military or social infrastructure (Maness and Valeriano, 2016). Taking this into account, stands the fear that a failure of deterrence can cause remarkable catastrophes even with a limited use of nuclear weapons – same as the Cold War era. Consequently, it becomes evident that the objective of a cyberattack is to usually cause disturbances rather than damage or destruction. In contrast, nuclear weapons are worldwide known as weapons of mass destruction and they forever pose a threat of prompt destruction. Last but not least, the price of a cyber operation is low and the game is available to anyone, from individuals to states (Owens et al, 2009).

Apart from the technical or political comparative attributes, the most important is the will to understand thoroughly this new developing technology and adopt the appropriate strategies to cope with any forthcoming challenges. Both nuclear weapons and cyberspace constitute revolutionary technologies in their time. Instead of simply implying that another revolution in military affairs has occurred, Valeriano and Maness argue that new technologies might require new tactics and without a doubt the support from older theories and established methods (2016). Rather than reinventing the wheel, it has been recognized that cyberattacks can illustrate the same potential as nuclear weapons in causing national insecurities. Nuclear deterrence was more complex than it first seemed, and this could easily be true for deterrence in the cyber domain (Geist, 2015). As Dorothy E. Denning cautions not to try to fit all cyber capabilities under the same strategy, suggesting "rather we need to narrow our treatment of deterrence as it relates to cyberspace." (2015, p.12). Denning moves on to recommend two feasible scenarios to the applicability of deterrence theory in cyberspace, one of which highlights the comparative attributes of cyber war and nuclear deterrence and the reconsideration of existing deterrence regimes to certain cyber activities (Ibid). The connection between cyber security and physical capabilities are said to welcome deterrence much easier (Goodman 2010). The important aspect of this observation remains the nexus between the two types of warfare.

3.7 Applying theory in practice – Cyber Deterrence

The emerging significance of cyberspace has already influenced the Westphalian state-based system in the international community. Among those impacts, one can notice the asymmetrical shifts in traditional power relations among states and the new opportunities for smaller actors to threaten stronger ones. At the same time, new diverse forms of cyber conflicts challenge the

stability and the security of a state, while more and more actors keep gaining power, either private and non-state commercial entities, individuals, novel criminal groups etc. All in all, the transformative effects of cyberspace undoubtedly spread throughout all levels of analysis in international relations, i.e. the individual, the state and the global system.

Respectively, the state is still the basic actor in international politics and except for all the new opportunities cyberspace created, there are also a few sources of threat. Many governments have used cyber venues to cater for social services, share information but also to pursue their own security by exerting their influence. This established behavior pushes for a more comprehensive view of national security, that could include the cyber domain. In this respect, recognizing that cyberspace is indeed one of the domains of warfare, the United States with the assistance of the U.S. Cyber Command have made efforts to centralize the command and coordination of cyber operations.[2]

This reality can only be understood through U.S. decision to militarize cyberspace. With this new policy paper, the DoD issued in 2018, some shift changes can be observed in the international system and more tensions are expected in the relationships among states. This too may be anticipated by the structural realist theory, yet with little insight about the potential outcome. More specifically, the U.S. dominance in the cyber realm, as well as the alarming ascending states, are largely consistent with the realist theory.

Realism can help explain the states behavior behind cyber arms racing as a response to threats in an anarchic international system. The security dilemma is also more critical when offensive and defensive capabilities are indistinguishable and states are unable to discern benign or threatening intentions (Jervis, 1978: 199-206). For realists, the acquisition of military capabilities is the key strategy to deterring aggression (Morgenthau, 1987). This international system is marked and determined by structural issues and relationships among states which at the same time are beyond the control of any individual (Pijovic, 2016). As already mentioned, the states are committed to anything that ensures their survival, and as a result more power. Bearing in mind that the United States are already regarded as one of the most powerful players in the

[2] According to the Department of Defense, the American government confirms the importance of developing counter cyber threat methods in order to develop the necessary protective system (DoD, 2015: 27).

international system, they should be in the position to maintain the status quo in their advantage, or else their distinguished place in global affairs (ibid).

The aforementioned theories have profoundly shaped the US cybersecurity doctrine. For instance, it has been illustrated that US strategists believe that the offense prevails over defense in cybersecurity, thus pushing them towards enhancing their cyber-offensive capabilities. In such an environment, anarchy and distrust is highly likely to be endemic. Consequently, states will be worried about other states' intentions, and tempted to protect themselves through offensive actions rather than relying on defensive systems. And since the manifestation of foreign policy is expressed through official policies, it is interesting to investigate how the US choose to legitimize their strategies. Multiple previous studies on the language of legitimation (van Dijk 2005; van Leeuwen 1996; van Leeuwen , 2007; van Leeuwen , 2008; van Leeuwen & Wodak 1999) have analyzed key strategies employed by social actors in their effort to justify their actions.

4 Methodology

This chapter justifies the selection of discourse analysis as a research method, while taking into consideration its qualities as an analytical tool. Further, the chapter examines the procedures followed through various stages of the research, which include the data collection through discourse analysis and the process of data analysis within the selected case study. For the purpose of this analysis, I chose to utilize an interdisciplinary framework, which constitutes a solid synthesis allowing to include the basic theoretical premises of discourse analysis and uses analytical tools from Systemic Functional Linguistics. This explanatory model introduced by Antonio Reyes (2011) revolves around the crucial use of language in society and how it is anchored to the legitimization process.

4.1 Research strategy

Under the scope of the aforementioned theoretical framework, the aim of this chapter is to describe the methodology used in the discourse analysis of this thesis. A qualitative research method was chosen as the backbone of the analysis in this paper as this approach reinforces the interpretation and the intentions of human interaction and politics. Undertaking a qualitative research enables to contextualize particular circumstances and gain a more in-depth

comprehension, under the guidance of specific concepts (Mack, 2005). Discourse analysis in particular offers a powerful toolbox for analyzing political communication. According to Fairclough (1992), "The methodology reason is that texts constitute a major source of evidence for grounding claims about social structures, relations and processes" (p. 211). This translates to the utility of discourse analysis to examine what is excluded in text, not only the obvious approaches. A qualitative study allows to examine issues that have not yet been addressed in their entirety, and in particular seeks to "asks how much a theory and a hypothesis can explain, how well it can explain it, or how meaningful and fruitful an explanation is" (Reiter, 2017, p.144).

As Denzin and Lincoln (2005) suggest, a qualitative research is holistic and emphasizes in the greater context. Furthermore, discourse analysis focuses on the contextual meaning of the language and emphasizes on the social aspects of communication. "The language we use both reflects and shapes the kind of world we create around us" (Strauss & Feiz, 2014, p. 1). This means that most forms of language could reflect the worldview of the writer and as Van Dijk mentions (2005), discourse analysis demonstrates how daily language is affected by ideologies. For instance, politicians seek to set guidelines, to meet their targets and obtain regulatory authorization over the decision-making process (Bayram, 2010). Language itself has no power assigned to it, but "language can be used to challenge power, to subvert it, to alter distributions of power in the short and long term. Language provides articulated means for differences in power in social hierarchical structures" (Wodak, 2001, p. 11). Nevertheless, "the connection between language and politics is strong as political action itself is carried out through language" (Bello, 2013, p. 86). Van Dijk affirms that "it is largely through discourse that political ideologies are acquired, expressed, learned, propagated, and contested" (2005, p. 732). More precisely, political discourse is concerned with political dominance, power abuse and legitimization of political phenomena (Bello, 2013; Fairclough, 1995). Ultimately, discourse analysis considers the context (social, political, etc.) within which the language functions, let alone the pattern and the structure of the discourse itself (Jalali & Sadeghi 2014; Van Dijk, 2003). Last but not least, a distinction between simple language analysis and discourse analysis clarifies that the latter does not regard language as an abstract system but rather views language as a communicative tool to pool information about memories and feelings (Eishenhart and Johnstone, 2008, p.3)

4.2 Strategies of legitimization in political discourse

As mentioned earlier, Reyes' interdisciplinary framework aims to explain specific ways in which language, words and semantics represent an instrument of control (Hodge and Kress, 1993, p.6). Drawing into previous studies on legitimization (i.e. Martin Rojo and Van Dijk, 1997; Van Dijk, 2005; Van Leeuwen, 2008) Reyes proposes some key strategies of legitimization which justify political actions and manifest symbolic power. This paper seeks to shed some light on the relationships between discourse and the manifestation of power in society, within the scope of critical discourse analysis. In this regard, this study will draw from Reyes's attempt to analyze linguistic patterns in which legitimization is constructed in discourse (p.785). Mainly, CDA practitioners utilize this method to interpret relationships between language and ideology, language and power and in this case I will utilize this analytical tool to decode the relationship between language and policy making.

As Reyes moves forward to analyze his research tool, he emphasizes the importance of linguistic choices employed in the message. For this reason, he explains that the best way to examine the linguistic representations of legitimization in discourse is to employ tools from Systemic Functional Linguistics (SFL). In his study, he considers and then further develops a set of categories initially proposed by Van Leeuwen (1996, 2007, 2008). These categories have been previously applied to the analysis of political discourse. Yet, Reyes builds up on these categories and provides a new context of comparison, which renders his framework an important auxiliary tool for this study by juxtaposing the way the current and former US presidents granted legitimization to their practices. Following, I will explain the theoretical foundations proposed by Reyes.

i. Legitimization through emotions.

The first strategy of legitimization that Reyes recognizes is based on the appeal of emotions. The positive/negative representation and the attribution of respective qualities allow the sender of the message to create both sides of the coin, separating the 'us-group' from the 'them-group'. In these strategies, legitimization is displayed through provoking emotions, particularly fear. Linguistically, this can be accomplished through 'constructive strategies' around this reference, what 'we' say or do, against 'the others' (Van Leeuwen and Wodak, 1999:92).

ii. Legitimization through a hypothetical future.

Another strategy in political discourse is linked to the future, our future which is threatened and thus, imminent action is required (Dunmire, 2007). Speculations about the future can be identified through specific linguistic choices and structures, such as conditional speech.

iii. Legitimization through rationality.

The legitimization is trusted when there's a proven heeded and thoughtful process that precedes it. In the literature, this strategy is referred to as 'Theoretical Rationalization' (Van Leeuwen, 2007). In this case of a policy paper, it is considered 'rational' to consult other sources and collaborate with every available department prior to decision making.

iv. Legitimization through voices of expertise.

The voice of experts is often recalled with the purpose to confirm and support an argument or a proposal with their knowledgeable statements in the specific field, i.e. the legitimization through authorization (Van Leeuwen, 2007).

v. Legitimization through altruism

Proposals tend to be legitimized when thought as a common good. "Institutional actions and policies are typically described as beneficial for the group or society as a whole' (Martin Rojo and Van Dijk, 1997: 528).

4.3 Case selection

By using a case study approach, the research "ensures that the issue is not explored through one lens, but rather a variety of lenses which allows for multiple facets of the phenomenon to be revealed and understood" (Baxter and Jack, 2008, p.544). This paper seeks to provide a multi-perspective analysis on whether radical policy shifts would foment feelings of insecurity in the international community.

The selection of these two cases is not based on random sampling. The United States hold great military, economic and soft power over the international arena. Attention will be drawn to two consecutive presidents, Barak Obama and Donald Trump, regarding cyber concerns. Since the US are among the great many countries that have declared the issue of cybersecurity as a national security threat and have developed cybersecurity strategies, this new development in their national security policies sparks great attention. At the same time, there have been

numerous cyberattacks of different consequences that have targeted the USA. In addition, the US constitute a great, highly securitized power within the international community, striving to ensure their sovereignty and dominance. Such initiatives generally outline a country's primary concerns and goals and it is thought-provoking to examine the actions taken. The following chapter helps to identify and examines the implementations that the US government has developed and bring them to the research.

After Barak Obama took office in 2009, his administration confirmed cybersecurity as a key issue and included it to the National Security Strategy. Next issued document, National Security Strategy 2010 stated the government's intentions to work on forming a more secure and sustainable cyber domain (Permik, 2016). During his presidency the Department of Defense issued a *Cyber Strategy* in April 2015 stating the three primary missions in terms of providing secure cyber space; defending the US network systems, defending the national interests against cyberattacks, and providing integrated cyber capabilities in order to support military operations (The Department of Defense Cyber Strategy 2015, p.4-5).One of the main strategic goals identified in this policy paper was to *"build and maintain robust international alliances and partnerships to deter shared threats and increase international security and stability".* This thesis' hypothesis, however, raises the concern that the cybersecurity strategy of the US has come a long way since Obama's policy implementations.

This paper analyzes the cases of former President Barak Obama's and current President Donald Trump's administration, especially the national cyber security policies. I will first explain the policy papers selected to justify the concern about the new balance of power in the global system. Following, I will refer to the analytical tools used to examine the selected documents and investigate how the behavior of the United States in cyberspace was justified under the Obama and later, Trump, presidency.

Since this process will be fulfilled by utilizing the method of discourse analysis, this chapter will also provide all the official terminology and policy settings that were considered under the scope of the analysis. It is important to identify the progress of the public discourse in parallel to the development of modern warfare. Even though the press has dedicated a lot of its attention to cyberwarfare, I will mostly refer to academic and political discourse so as to obtain an objective view on the issue. The main document under examination is the unclassified DoD's

Cyber Strategy that was issued in 2018 in direct correlation with the Cyber Strategy published in 2015. Those two official policy doctrines were drafted under different administrations. My goal is to indicate the military's role under the two cybersecurity policies. The discourse analysis of a security policy document aims to examine how various test and language elements are building up each other and the text in its whole. Furthermore, the analysis will examine how the policy document intends to influence the regulated practice and behavior of states in the international arena.

In addition, the full document of the US national cybersecurity policy proposed by both administrations will be reviewed in order to establish a broader context under which the military forces are to operate. The reason lies within the fact that a national security strategy constitutes the "only complete whole-of-government national security document that the U.S. Government publishes" (Stolberg, 2013, p,73). Under this light, this strategic document serves mainly as an umbrella for other lower level policy documents (ibid). The premise of this analysis is primarily the national and transnational cyber strategies and how these are framed through state representatives and policy makers asserting cybersecurity to be an important issue of national and civilian security. Furthermore, this analysis is limited to unclassified and open source information.

Policy documents offer an abundant resource for policy analysis, that is how and why governments enforce certain policies (Browne, Coffey, Cook et al, 2018). The main concern of this research is the way that policies materialize and how policy problems emerge (Blackmore & Lauder, 2005; Fisher, 2003). The need to examine the effects of policy processes is urgent for the maintenance of the anarchic international system.

4.4 Validity and reliability

In a project as this thesis, apart from a clear methodology, the validity and reliability of the data gathered will be elaborated on as well. Reliability is referred to the stability of findings, whereas validity is represented the truthfulness of findings (Altheide & Johnson, 1994). Validity and reliability increase transparency, and decrease opportunities to insert researcher bias in qualitative research (Singh, 2014).

On the one hand, validity refers to the extent of which a test measures what we actually wish to measure, whereas reliability refers to a measurement that supplies consistent results.

(Blumberg et al., 2005). First and foremost, the research conducted is valid when able to answer to the research question. In addition, since the literature on the topic of interest is rather scarce, the author of this thesis used an already established theoretical framework, in order to ensure the validity of the research. Finally, when discussing matters of reliability, previous research has established that both findings and data are to be seen as reliable when multiple research yield identical results (Ali and Yusof, 2011). In the aspect of qualitative research specifically, in order to attain reliability, "there is a need for the qualitative researcher to document the succession of moves through the stages of data production, analysis and interpretation" (ibid, p.35). A thesis is considered reliable when it reflects consistency and replicability over time (Fraenkel & Wallen, 2003; McMillan & Schumacher, 2001, 2006; Moss, 1994; Neuman, 2003). Messik (1989) has accepted a unified concept of validity which includes reliability contesting that an argument must be relevant and able to be utilized in a reliable manner. The purpose of establishing reliability and validity in research is essentially to ensure that data are sound and replicable, and the results are accurate. In this respect, one may argue that the methodology and analysis of the present study guarantee such a process.

5 Analysis

This chapter investigates the discursive strategies employed in discourses by the political leadership to legitimize their ideological views and actions. It begins with an observation of the overall similarities and differences between the two main documents, i.e. the 2015 and the 2018 Department of Defense (DoD) Cyber Strategy, and proceeds with the discursive assessment following Reyes' legitimization strategies.

5.1 General Observations

5.1.1 Obama's cybersecurity legacy

President Obama devoted considerable resources and energy to make cybersecurity a priority in his political agenda and a key topic in almost every State of the Union address. The administration laid out the traditional government markers of careful policy consideration and development as attempts to establish a more aggressive cyber doctrine was highly likely lead to amplification of any worries and fear over the militarization of the internet. The 2015 cyber strategy was, for this reason, a more comprehensive articulation of the DoD's role in defending the United States and how the DoD would integrate US cyber capabilities into military operations.

The strategy identifies the three key missions for the DoD, summarized as: (1) defending its own networks, systems, and data; (2) defending U.S. national interests against cyberattacks of "significant consequence," including loss of life, significant damage to property, serious adverse U.S. foreign policy consequences, and serious economic impact; and (3) when directed by the President or Secretary of Defense, supporting military operations and contingency plans with cyber operations, including by disrupting an adversary's military-related networks.

On its whole, the 33-page document was transparent, revealed all the steps needed to fulfil the strategy, and focused mainly on deterrence and innovation. Former Secretary of Defense (SECDEF) Ashton Carter considered the general public important when he clearly stated that this strategy is *"also a reflection of DoD being more open than before"*(Carter, 2015). Here appears clearly the willingness of the DoD to become more transparent about US military doctrine, policy and missions in cyberspace. In that sense, attempts such as better information to the public and enhanced declaratory policy in the cyber domain are portrayed. A more noteworthy aspect to point out is that the DoD plays a more significant role in defending the

homeland and private companies. This assertion is supported by the 2015 strategy's introduction which is as follows:

> *In concert with other agencies, the United States' Department of Defense (DoD) is responsible for defending the U.S. homeland and U.S. interests from attack, including attacks that may occur in cyberspace. In a manner consistent with U.S. and international law, the Department of Defense seeks to deter attacks and defend the United States against any adversary that seeks to harm U.S. national interests during times of peace, crisis, or conflict (2015, p.2).*

The strategy seeks to provide the necessary tools for citizens to protect themselves, companies to defend their information, and the governmental authorities to protect civilians from harm. The 33-pages document, through a collage of initiatives, appears to provide a prioritized approach to the hurdles of applying limited resources to the ever-growing challenges of cyberspace (DoD, 2015). The document's conclusion, however, arrives at a statement that offers no priorities and offers a vague statement about the future. While the 2015 cyber strategy might seemingly not offer any significant background to what the DoD has been implementing prior to April 2015, its purpose remains explicitly clear throughout the document (p.3, 2015). The document aims to be the expression of stated principles of the US government. More specifically, the word "doctrine" appears twice in the document, yet not in a sense that serves the operational implementation of the strategy. In other words, it fails to elaborate extensively on how exactly the government seeks to implement this strategy. For instance, it mentions:

> *To ensure that the Internet remains open, secure, and prosperous, the United States will always conduct cyber operations under a doctrine of restraint, as required to protect human lives and to prevent the destruction of property. (p. 6)*

> *[…] to bring greater understanding and transparency of each nation's military doctrine, policy, roles and missions in cyberspace. (p. 28)*

It appears that the 2018 strategy represents a thoughtful maturation of the US cyber strategy. Albeit it reflects the administration priorities and the realities of the international political environment, there are still challenges to the implementation of the strategy that allows for a more deliberate translation.

5.1.2 Trump's forward defense

The six-page summary document outlines the military role in cyberspace in the context of the Joint Force – i.e. Army, Navy, Air Force, the Marines, and the Coast Guard. It also describes the three main guiding operational concepts, namely intelligence gathering (valuable information about allies' and adversaries' activities), conflict preparation (activities that ensure the battlefield arrangements), and defense forward (independently interpreted as activities that halt attacks before they reach US infrastructure and networks). [3]

In general, the 2018 Cyber Strategy reflects developments in the political environment and the need to address these changes effectively. For instance, Over the last three years, more sophisticated cyber attacks have taken place, the Russian campaign which allegedly aimed at disrupting the US presidential elections in 2016 being one prominent example. Newly developed foreign policy, relying further on great-power competition, was also closely aligned to an evolving domestic political landscape. Specifically, it seems that the Trump administration has adopted a more risk acceptant approach. [explain more, or mention earlier] The recantation of the Obama-era presidential directive on response to cyber activities (PPD-20) stands as validation for this new more risk-tolerant approach. As Bryson Bort, CEO and founder of SCYTHE remarks "up to this point, deterrence was a concept with no teeth. Now, we've added teeth" (Rashid, 2018).

The new cyber strategy can be summarized into the following three central tenets: great power strategic competition, defend forward, and prepare for war. This means that America is prepared to respond offensively, as well as defensively, in cyberspace. At first glance, the new strategy is more focused and more active than its 2015 predecessor. It centers on foreign governments' attempts to target and attack US networks -namely China and Russia, given that they have been the main strategic adversaries to the United States over the past decades- who demand actions with a strategy that aims to preempt, counter, deter and ultimately prevail. All in all, the new strategy follows the footsteps of the 2015 document towards a free and open internet for everyone. Nevertheless, it appears that, through the newest policy developments, the United

[3] "We will conduct cyberspace operations to collect intelligence and prepare military cyber capabilities to be used in the event of crisis or conflict. We will defend forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict,"

States have officially rendered standard preparations for defense obsolete and now decided to confront their adversaries before they initiate an attack against them.

The introduction of a new mission to "defend forward" is probably the most significant aspect of the 2018 strategy. The term illustrates the more active and more offensive tone of the strategy. While the 2015 strategy calls on the DoD to "be prepared to defend the US homeland and US vital interests"(DoD 2015, p.8), the 2018 strategy orders US forces to "defend forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict (DoD 2018, p.1). This newly introduced concept is in interesting in multiple levels. Firstly, it is intriguing for an official policy paper to introduce a new term without providing a fully developed definition. The *DoD Dictionary of Military and Associated Terms* entails the official US military and associated terminology to improve communication within the DoD and other governmental components.[4] Normally, since the term is associated with the law of conflict and warfare, *jus in bello*, one might argue that it should be articulated with precision and in accordance with the international law. When assessing and establishing an official policy, it is important to develop a full understanding of how a term may be defined or used.

Alarmingly, the strategy places defense beyond the military networks and instead involves operations beyond the military, even in the private sector. This is interesting for the following reasons. Initially, deterrence of cyber activities does not have to be embodied solely in cyberspace. The strategy advocates defense of resources and infrastructure which enable operations "across the full spectrum of conflict" (p.1). This statement implies that the restraint in cyber operations witnessed under the Obama administration will no longer be preserved under Trump's operations. All in all, this shift from reactive to preemptive strategy marks the most significant evolution from the previous cyber strategy and comes in response to repeated cyber campaigns directed by US adversaries, such as China and Russia.

The strategy also expands geographically, i.e. beyond the US boundaries, by instructing forces to halt adversary activity at its source. That is, deterring threatening cyber activities *before* these affect US networks and integrity. With a quick interpretation of this geographical elasticity, operations could now be carried out through counterintelligence activities instead of simply

[4] Office of the Chairman of the Joint Chiefs of Staff, DOD Dictionary of Military and Associated Terms, (Washington DC: The Joint Staff)

building walls around networks. This information presumably could be intelligence about conventional order of battle and military activity, cyber capabilities or any other valuable piece of information, either related to cyber activities or not. The opening phrase of the 2108 strategy confirms it:

> *American prosperity, liberty and security depend upon open and reliable access to information (2018, p.1).*

As a consequence, this means that, "defend forward" introduces a more preemptive response rather than a reactive one to potential enemy advancements. This new approach leaves many questions regarding its materialization and execution, which the DoD fails to answer in this released summary.

In this section, I mentioned briefly the key concepts and introduced the new environment where the 2018 new cyber strategy was presented. Following, Table 1 offers a comparison of both documents' strategic objectives.

The DoD Cyber Strategy 2015 Strategic Goals	*Summary, DoD Cyber Strategy* Objectives
I. Build and maintain ready forces and capabilities to conduct cyberspace operations.	I. Ensuring the Joint Force can achieve its missions in a contested cyberspace environment.
II. Defend the DoD information network, secure DoD data, and mitigate risks to DoD missions.	II. Strengthening the Joint Force by conducting cyberspace operations that enhance U.S. military advantages.
III. Be prepared to defend the U.S. homeland and U.S. vital interests from disruptive or destructive cyberattacks of significant consequence.	III. Defending U.S. critical infrastructure from malicious cyber activity that alone, or as part of a campaign, could cause a significant cyber incident.
IV. Build and maintain viable cyber options and plans to use those	IV. Securing DoD information and systems against malicious cyber

options to control conflict escalation and to shape the conflict environment at all stages.	activity, including DoD information on non-DoD-owned networks.
V. Build and maintain robust alliances and partnerships to deter shared threats and increase international security and stability.	V. Expanding DoD cyber cooperation with interagency, industry, and international partners.

Table 1. The strategic goals of the 2015 and 2018 cyber strategies

5.2 Application to Reyes' framework

i. Emotions

As already mentioned in the methodology chapter, the first legitimization strategy relies on the appeal of emotions. In other words, this means that social actors evoke various types of emotions in order to legitimize their actions or words and thus prompt a standard behavioral response. In that sense, emotions appear to be often manipulated for the facilitation of the political agenda (Reyes, 2010). Expressing emotion enhances intimacy and brings the one who wants to convey a message closer to the addressee. It can be fairly considered as a very important aspect of the legitimization strategy, since it lays the ground for understanding (Reyes, 2011). Essentially, emotions skew the audience towards accepting any given proposal by the social actor, who deliberately triggered those emotions initially.

Reyes himself points out that the emotion of fear in connection to the past and future incidents could be the right emotion to demonize the enemy (2011). More specifically, in order to stir up fear and anxiety while constructing 'them' as the enemy, there must be a prominent juxtaposition with the fate of 'us' and how the latter is endangered by the enemy's illegitimate power.

In the following excerpt, the 2018 policy paper is linguistically reconstructing the antithesis between the enemy 'them' by emphasizing the 'us'. This juxtaposition involves not only the United States but also their allies and the need to protect against unacceptable risks.

(1) Competitors deterred from engaging the United States and our allies in an armed conflict are using cyberspace operations to steal *our* technology, disrupt *our* government and commerce, challenge *our* democratic processes, and threaten *our* critical infrastructure (p.1).

ii. A hypothetical future

According to Reyes, legitimization can also occur following a timeline that connects the past, with the present and, logically, the future (Reyes, 2011). His second strategy is *legitimation through a hypothetical future*, where a past challenged is invoked to legitimize an imminent action to avoid a future repetition of the same challenge. Consequently, political actors use this timeline to their advantage and declare the present as a period that calls for crucial decisions and fruitful resolutions (Ibid). There can be two alternatives presented by the political actor. The first one describes what will happen in the future "if we do not do what the speaker proposes in the present" and the second alternative describes the contrary scenario of what will happen "if we do act according to the speaker's suggestion" (Reyes 2011, p. 793). The following examples demonstrate how this strategy can be portrayed in the documents:

DoD 2018 Cyber Strategy
(2) "[w]e must ensure the U.S. military's ability to fight and win wars in any domain, including cyberspace (p.2).
(3) "Should deterrence fail, the Joint Force stands ready to employ the full range of military capabilities in response (p.4).
(4) We will conduct cyberspace operations to collect intelligence and prepare military cyber capabilities to be used in the event of crisis or conflict (p.1)
(5) Taken together, these mutually reinforcing activities will enable the Department to compete, deter, and win in the cyberspace domain (p.7).

DoD 2015 Cyber Strategy
(6) A disruptive, manipulative, or destructive cyberattack could present a significant risk to U.S. economic and national security *if* lives are lost, property destroyed, policy objectives harmed, or economic interests affected (p.2)

(7) It works by convincing a potential adversary that it will suffer unacceptable costs *if* it conducts an attack on the United States, and by decreasing the likelihood that a potential adversary's attack will succeed (p.11).
(8) *If* directed, DoD should be able to use cyber operations to disrupt an adversary's command and control networks, military-related critical infrastructure, and weapons capabilities (p.14).
(9) If and when U.S.-Russia military relations resume, as a part of broader interagency efforts DoD will seek to develop a military-to-military cyber dialogue with Russia to foster strategic stability in cyberspace (p.28 footnote).

iii. Rationality

The legitimization strategy of rationality seeks to demonstrate the action-taking process of the policy that concludes as a result of a heeded and thoughtful procedure. In other words, legitimation by reference to the natural order of things (Reyes, 2011). Rationality is introduced as a social construct that represents what is right and what is wrong in a given society and is accomplished by representing decision making as a thoughtful and careful process that leads to a final, rational decision. In addition to this, it is worth remarking that, as Reyes points out, what is right and wrong might depend on variables such as ethics and subjectivity. However, rationality in the context of this paper is based on those values and morals that are recognizable within the community.

In the following examples, I display the way social actors exploit rational constructs in their effort to justify any actions taken. It is the very nature of the internet and its interconnected networks that have supported the U.S. military and upraised its dominance in the warfighting domains. In their turn, the States, need to protect the very nature of the internet, as we observe in the following excerpt:

(10) Computers and network technologies underpin U.S. military warfighting superiority by enabling the Joint Force to gain the information advantage, strike at long distance, and exercise global command and control (2018, p.1)

(11) We are vulnerable in this world. […] The Internet was not originally designed with security in mind, […] Without strong investments in cyber defenses […] malicious actors […] can use cyber capabilities to strike directly at a network

thousands of miles away, destroying data, disrupting businesses, or shutting off critical systems (2015, p.1)

iv. Voices of expertise

The fourth strategy identified by Reyes *voices of expertise* "are displayed in discourse to show the audience that experts in a specific field are backing the politician's proposal with their knowledgeable statements." (Reyes 2011, p. 786). In this respect, according to Reyes, legitimation can be realized through reliable sources, numbers or personal experiences (Reyes 2011, p. 787). As such, the cyber incident of Sony is mentioned as a collective personal experience that affected a large number of the population. It explains how a serious attack that affected a big company could easily affect everyone (civilians) in every aspect of their lives. Further, it legitimizes any future actions based on the argument that all the necessary precautions and actions are taken. The argumentation of the 2018 paper, consequently does not simply mention catastrophes and doom scenarions. In contrast to the 2018 strategy which lacks in examples personal experiences.

(12) The North Korean attack on Sony was one of the most destructive cyberattacks on a U.S. entity to date. (2015, p.2)

(13) Through years of practice and exercise, a culture of resilience took root in the military and units were ready and prepared to operate in contested environments (20115, p.4)

(14) For example, the United States military might use cyber operations to terminate an ongoing conflict on U.S. terms (2015, p.5)

(15) network service providers across DoD must be adaptive and active to follow cybersecurity *best-practices*

(16) For example, the United States used verifiable and attributable data to engage China about the risks posed by its economic espionage 2015, p.12)

v. Altruism

Reyes's last legitimation strategy is *altruism.* This strategy presents actions as beneficial for the community and avoids judgement about personal interests and selfishness (Reyes, 2011). It is

important to point out that self-interest is not an acceptable motive for political actors. Rather, the practices are made to look like a service that considers the wellbeing of others.

(17) the United States will always conduct cyber operations under a doctrine of restraint, as required to protect human lives and to prevent the destruction of property (2015, p.6)

(18) DoD will work with key Middle Eastern allies and partners to improve their ability to secure their military networks as well as the critical infrastructure (2015, p.26)

There are no similar excerpts in the 2018 strategy. In the contrary, there are clear mentions of US interests and superiority, such as in:

(19) We will strengthen the security and resilience of networks and systems that contribute to *current and future U.S. military advantages.* We will collaborate with our interagency, industry, and international partners to *advance our mutual interests* (2018, p.1)

In this section I have introduced the strategies of legitimation identified by Reyes in his study of legitimation in political discourse and have utilized them in order to analyze the two cyber strategies of the US Department of Defense. As it will be argued in the following chapter, the difference in the language used is evident. While the 2015 strategy is more meticulous and elaborative, the 2018 struggles barely to introduce its new concepts in a more attentive and reasonable manner, so as to ensure their justifications. Next, I discuss further the content of the aforementioned strategies and how they portray the US posture in cyber space.

5.3 Analytical Repercussions – what has changed and what remains the same

As already mentioned, the new strategy document is decidedly more risk acceptant and forward leaning that its predecessor. What follows in this chapter is a more analytical approach regarding the key concepts introduced in the said document.

The Presidential Policy Directive 20, which was issued by the Obama administration, set in place processes and procedures that required approval by the President or the Secretary of Defense before any government agency could launch an attack in cyber space. This served the purpose of containing any possible escalation of cyber activities. However, Trump's

administration evidently condemns this Directive and grants authorization for cyber attacks to the Department of Defense and its officials. Rescinding the older rules that required interagency coordination before finally the launch of an operation seems to enable the US to operate more quickly. Superseding the PPD-20 brings the responsibility of a new attack to the authority of the DoD commanders and away from the higher ranks, such as the President himself. Explicitly, in the 2018 document it is quoted that the DoD personnel will be *"held accountable for their cybersecurity practices and choices"* (p.5). On the contrary, the 2015 strategy clearly specifies that the US military may conduct cyber operations *"if directed by the President or the Secretary of Defense".* Another ambiguity under this claim is the use of the word "when". The Department is called for being prepared to defend and protect the US interests "when" directed (p.2) and "when" authorized (p.3), without further explanation on who authorizes the procedure to be followed. At this point it becomes evident that the authorization of cyber operations falls further down in the center of command on the hands of officials.

Another point worth mentioning is the state behavior in cyberspace. According to the goal of the 2018 document is to strengthen alliances and partnerships to ensure mutually supporting cybersecurity activities (p.5). What is intriguing in this statement is the distinction of the state behavior in cyberspace "*during peacetime"(ibid)*. One could say that Trump administration is trying to loosen the legal norms of state behavior during war and during peace and justify the same behavior during war as well.

Another aspect of state behavior is the relationship with allies and partners. The strategy declares that the US allies' capabilities will be used in a way that would complement their own (p.5). However, the DoD's ability to *"leverage"* its partners' and allies' capabilities could be ambiguously interpreted. This choice of word is especially interesting, as it comes in direct contrast with the *"trusted relationships"* they seek to build with their partners. While this paper is justifying any collaboration and utilization of partnerships during peacetime, it simultaneously suggests that the Department will *"reinforce voluntary, non-biding norms of responsible state behavior"* (p.5). This leaves a lot to be interpreted so as to what type of behavior is expected from the United States towards their allies in the event of war or conflict of interest. Later on the conclusion, *allies* and *competitors* are mentioned in the same sentence and are both expected to

abide with the US vital interests. Conclusively, the 2018 treats allies and adversaries equally, without distinguishing the behavior towards them.

Another contrast is that the 2015 document illustrates much more examples from the past. It mentions the government response that was observed following the Sony incident. This example constitutes a recent incident that shook the American community and which is utilized to emphasize the vulnerability effect in cyberspace on every citizen. The lessons learned from this incident are used to highlight the imminent threat against public safety and every other aspect of private life, such as the economy, health, education, telecommunications etc. Using real examples and lessons learned from the past outweighs the utilization of invoking fear, an emotion plays a leading role in the 2018 strategy. Legitimation does not rely solely on creating the emotion of fear through images of destruction and danger but lays out a situation with a logical sequence, which allows the reader to identify with and understand the problem. At first glance, the new DoD's strategy is far more offensive in nature and allows the US to assertively take any necessary measures in order to respond to any adversary as they *cannot afford inaction. (p.2, 2018),* whereas the 2015 policy is more diplomatic and defensive and mentions that *[a]s a matter of principle, the United States will seek to exhaust all network defense and law enforcement options to mitigate any potential cyber risk to the US homeland or US interests before conducting a cyberspace operation (p.5, 2015).*

Albeit the changes that have occurred in the two documents, a number of common factors remain. First and foremost, both strategies acknowledge the free and open internet as a foundational objective for US strategy. *The United States is committed to an open, secure, interoperable and reliable internet that enables prosperity, public safety and the free flow of commerce and ideas (p. 1, 2015).* They both accept also that in the same time: *[T]he arrival of the digital age has also created challenges for the Department of Defense (DoD) and the Nation. The open, transnational, and decentralized nature of the Internet that we seek to protect creates significant vulnerabilities. (p.1, 2018).* This similarity corroborates a well-established belief that *American prosperity, liberty, and security depend upon open and reliable access to information.* (p.1, 2018). Even though the two administrations stand in different positions on the role of the United States in the international system, they seem to maintain this same belief; the United States' commitment to an open and secure Internet.

Both strategies highlight the need to enhance resilience and increase defense capabilities in cyberspace to ensure the United State's superiority in the warfighting domains. Both acknowledge that *[t]he Internet empowers us and enriches our lives by providing ever-greater access to new knowledge, businesses, and services (p. 1).* In addition, the two strategies underscore the need to cultivate and *enhance the Nation's cyber talent (p.6, 2018)* and *build a cyber workforce […] to help achieve many of the objectives entailed in the strategy (p.17, 2015).* Lastly, both documents recognize the importance of strengthening alliances and attracting new international partnerships in order to "*deter shared threats and increase international security and stability" (p. 26, 2015).* Generally, the two documents fail to provide with specific guidelines. Besides, such documents are expected to articulate mostly the broad spectrum of the main threats to national security aligned with some rough themes and objectives about the government's course of action. [reformulate for stronger impact]

Yet, despite these commonalities, one should not disregard significant differences in the two documents that evidently lead to different behaviors, and consequently, different responsibilities in cyberspace. The most striking one could be the essence of each document. The 2015 strategy highlights the DoD's efforts to *mitigate risk* and *control escalation (p. 7, 26).* In comparison, the 2018 strategy is much more proactive, pledging to *defend forward to disrupt or halt malicious cyber activity at its source and to assertively defend [their] interests. (p.1-2)* This is highlighted by the notion that *[t]he United States cannot afford inaction: our values, economic competitiveness, and military edge are exposed to threats that grow more dangerous every day (p. 2).* Additionally, the 2018 document seeks to ensure that the US military can and will win in each warfighting domains, including cyberspace (p.2). Another dissimilarity is the emphasis in the 2018 strategy's changes on the dod's missions, including pre-emption and active defense. As White House National Security Advisor John Bolton mention in a press conference "We will identify, counter, disrupt, degrade, and deter behavior in cyberspace that is destabilizing and contrary to national interests, while preserving the United States' overmatch in and through cyberspace") (Nakashima, 2018). In contrast, in the 2015 strategy, these priorities included the preparation of defense of the States and *if directed by the President or the Secretary of Defense, dod must be able to provide integrated cyber capabilities to support military operations and contingency plans. (p. 5).* On the other hand, the 2018 strategy advocates for more expansive actions and permits the employment of *offensive cyber capabilities […] that allow for the use of*

cyberspace operations across the full spectrum of conflict (p.1). Particularly, the new strategy codifies the ability of agencies like the NSA and other military branches to conduct offensive operations proactively. Further discussion on the aspects of retaliation through hacking-back, will follow in the next chapter.

Taking a more careful look one might notice some interesting differences in the use of language. Precisely, the use of the word *"competition"*aligns with the National Security Strategy (2017, p.27-28) in reference to China and Russia. The 2018 mentions these two countries explicitly in its introduction and draws all the attention on these *"states that can pose strategic threats to US prosperity and security"* (p.1). More specifically, the document calls out China for cyber-enabled attacks that targeted the economic and intellectual property of the US in the past. Next, it mentions Russia's intent to destabilize and challenge their democracy (p.1) This mention leads to a logical justification of the DoD "*prioritiz[ing] securing sensitive DoD information and deterring malicious cyber activities that constitute a use of force against the United States, our allies, or our partners"* (p.4). Furthermore, the strategy does not fail to mention that, whereas the US tend to view conflicts through the binary lens of war or peace (Pomerleau, 2018), their competitors, such as the aforementioned, seem constantly engaged in war, with efforts *"to include persistent campaigns in and through cyberspace"* (p.1). In addition to the emphasis on the word "persistent" (p.1, 4) the strategy highlights the constant nature of the competition as well as lays the ground for a steadfast strategy based on constant operations *"to fight and win wars in any domain, including cyberspace"* (p.2)

On the other hand, the 2015 strategy refrains from the word *"competition"* to describe the relationship between not only China and Russia but also Iran, North Korea, ISIL and non-state actors (p.9). This renders the 2015 strategy a more comprehensive deterrence strategy, which might have incorporated response operations against a wide range of cyber activities without declaring as a constant competition. White House national security adviser John Bolton was reported saying that the main goal of this aggressive deterrence strategy is not to allow more offensive operations in cyberspace, *"but precisely to create the structures of deterrence that will demonstrate to adversaries that the cost of their engaging in operations against us is higher than they want to bear*".

Finally, the 2018 strategy concludes with a clear forewarning for the Pentagon's intentions to *"prepare for war"*, a word which is avoided in 2015. Combined with the intention to *"build a more lethal force"* (p.4) this statement adds to the holistic competition rhetoric of the National Security Strategy and the DoD's cyber strategy. Nevertheless, preparation for war could also be interpreted through the lens of emergency for incorporating cyber operations within the whole warfighting domain or even to underline the emerging vulnerabilities inherent in the US networks. The 2018 document specifically mentions the use of active cyber defense capabilities to prevent potential attacks and intrusions. The use of kinetic military force in response to a cyber attack is the ultimate expression of active cyber defense. Cyberspace might have already been classified as the fifth domain of warfare states, such as the USA and Japan (Japan, 2013), but adopting such active defense policies enhances the militarization of security.

In this chapter, I unraveled some of the key terms and concepts mentioned in both the DoD cyber strategies, namely defend forward, day-to-day competition as well as sought to assess the legitimation process of the 2015 and 2018 cyber strategies in reference to the framework determined by Reyes. It appears that the 2015 entail more meticulous and academic language and structure, as it does not fail to include different types of legitimation to establish credibility. On the other hand, the 2018 strategy, in combination with Reyes's framework illustrates the impulse and provocative stance of Trump administration. In the following chapter, I will proceed with analyzing my findings with respect to the international relations theories pinpointed in my theoretical chapter.

6 Discussion

The present thesis aimed to observe how the newly adopted cyber strategy by the Department of Defense and its overall offensive posture will affect the status quo both in the cyber and in the international domain. The US is undoubtedly a superpower in the world of politics and technology and their perspective on cyber space could have a great impact for other players in the international system. For this reason, it was important to investigate the presidents' use of legitimation strategies.

In addition to answering these questions by relying on document analysis, this paper drew on international relations theories. The theoretical background included both the realist approach of international relations, and the concept of balance of power and the maintenance of the status quo, as well as deterrence theory. Most prior research regarding cyber conflict examines whether or not deterrence theory could be applied on cyber weapons same as it did on nuclear weapons. Other researchers' work revolves around the question whether or not a new cyber Cold War is possible. This thesis relied on the argument that deterrence theory is indeed applicable on cyber space and aimed at drawing attention to the possible strain put over the diplomatic relations of nation-states, as a great power adopts a more offensive stance in the digital domain.

To answer the main research question, to what extent is the US Cybersecurity Strategy precipitating a security dilemma and how has the US government legitimized its strategy since 2015, I analyzed the two policy papers published by the Department of Defense under two different administrations, Obama and Trump. The section analyzed both presidents' use of legitimation strategy according to the Reyes's typology. Examples of all legitimation strategies, i.e. through (1) emotions (particularly fear), (2) a hypothetical future, (3) rationality, (4) voices of expertise and (5) altruism, were found in the cyber strategy under the Obama administration. As for Trump, the 2018 cyber strategy appears to be rather poor in legitimation strategies, other than the use of emotions. Obama's administration aimed to legitimate its future actions in cyberspace while acknowledging the threat environment around the United States, but still chose to focus on the positive side and refrain from drawing too much attention to the possibility of a cyber war. On the contrary, Trump aims to justify why the US should be more proactive and offensive in cyberspace and thus maintain their superiority in all warfighting domains. The 2018

strategy focuses mostly on the behavior of the major US adversaries and how the United States should always be steps ahead.

Overall, the differences between the two presidents' use of the legitimation strategies are more evident that the similarities. Under the Obama administration the issued document was freely available to the general public, was more extensive and relied on solid argumentation and breakdown of the strategy. In contrast, the whole document under Trump's presidency remains confidential, does not exceed five pages and is rather repetitive than informative.

As already mentioned, the US public policy discourse has been framing cybersecurity using analogies of war. The present paper argues that catastrophic doom scenarios have been a consistent pattern of US cybersecurity policy discourse and questions whether this dominant thinking about cyber conflict would ultimately tip the scales of the balance of power in cyberspace. Looking back at the theoretical framework of analysis within the International Studies it becomes clear that the offensive character of the 2018 strategy suggests that the Obama administration catered for preserving the status quo, whereas Trump's Department assumes the status quo is already challenged and thus drastic measures are needed.

6.1 Threat environment

In order to dwell deeper in the discussion, the threat environment needs to be outlined. The applications of information technology (IT) far exceed interconnectedness and information sharing. To this day, IT has evolved from an administrative tool for enhancing operational effectiveness into a national strategic asset. The high-profile and state of the art digital infrastructure now offers the United States critical advantages over any other political power. However, this can be both a blessing and a curse. Its reliance on computer networks, at the same time, could also enable potential adversaries to gain valuable intelligence about US capabilities, to infiltrate US networks and disrupt US economy and life. For the US to hold their throne in the international system, they need to understand that cyberwarfare entails attributes of maneuver warfare. To maintain their advantage the United States need to constantly adapt to the circumstances quickly and improve their defenses (Lynn III, 2010). Thus, the US government needs a strategy that can provide operational flexibility and cyber capabilities that offer maximum adaptability in the fifth domain.

In the aftermath of the cyber strategy that the Trump administration introduced in 2018, defending forward has been made possible by consolidating the Defense Department's collective cyberdefense capabilities under a single roof and by linking them with the signals intelligence needed to anticipate intrusions and attacks. The speed at which active defense systems must act in the event of an attack means that the rules of engagement governing network defense must be set largely in advance. These rules of engagement will then have to determine what action is necessary, appropriate, proportional, and justified in each particular case based on the laws that govern action in times of war and peace. In this interpretation, it becomes evident that in order to assure national safety in cyberspace, both powerful and highly vulnerable states like the US, China or Russia must anticipate attacks far forward than their occurrence as well as be able to impede the threats that indeed manage to penetrate. All states, in one way or another, will try and determine what they fear from the internet (the lack of sovereign control over what comes through their borders).

US officials have been quoted in multiple occasions praising the new orders for an offensive step forward as adding flexibility and offering an advantage to their behavior in cyberspace (Rudesill, 2018). This argument is based on the notion that a good defense requires the ability to successfully operate offensively, knowledgeably, and rapidly in order to pro-actively preempt an attack (Demchak & Dombrowski, 2011). However, there are some drawbacks to this risk-acceptant cyber strategy. As the 2015 focused more on the fear of escalation in the event of US response operations rather than from adversary activities, the 2018 strategy recognizes the risk and the threat stemming from China and Russia. As a result, the US frames risk in a way that allows for a more effective deterrence strategy and a more ‘offensive’ defense. Let alone, the focus on degrading adversaries’ cyber capabilities instead of threatening with attacks, avoids escalation but operates in the dark paths of counterintelligence and not head on confrontation. In that sense, such operations can occur below the threshold of conflict but still threaten the status quo.

Martin Libicki, a professor at the US Naval Academy, mentions that granting DoD staff and officials the authority to launch cyber attacks as retaliation could easily turn the internet into a ‘free-fire zone’(Libicki, 2009). This approach leads to the impression that the US administration is looking for a way to strike back to its adversaries and is simply trying to loosen

the legal restrictions. The evident focus on the use of offensive tools for the sake of retaliation has been worrying academics and experts. Undoubtedly, the United States is one of the most wired global economies, whose communications, technology, energy domains and much more are reliant on the internet, and thus, is also very much vulnerable to cyberattacks. In that sense, committing to retaliation disregards the greater responsibility and abiding interest of the United States in encouraging stability in cyber space. Other nations also possess strong cyber capabilities or are working their way into developing them. Hence, the US government should take a step back and reconsider the precedents it will set when using these capabilities and the shift balance it will cause in the anarchic international system.

6.2 Parallels to the Cold War

In 1940s Japan humanity witnessed the worst outcome of nuclear weapons. In contrast to the military field, the worst scenario in cyberspace is rather ambiguous and easily predicted. In cyber, many are reluctant to use cyber weapons for fear of effectively being a weapon of mass destruction. This thesis, along with an ever-growing number of voiced opinions, argues that cyber weapons will nevertheless be employed successfully with more localized and reversible effects than nuclears. In other words, cyber weapons can be used as weapons of discriminate disruption which can be leveraged to their advantage.

General Fang Fenghui, Chief of General Staff of the People's Liberation Army of China mentioned that if the security of the internet cannot be monitored then "it's not an exaggeration to say the effects could be no less than a nuclear bomb"(Bloomberg news, 2013). Evidently, General Fang is not the only one drawing these comparisons. Secretary of State John Kerry once responded in his hearing that [he] could call [cyber weapons] the 21st century nuclear weapons equivalent (Kerry, 2013). At the same time, Russian Deputy Prime Minister Dmitry Rogozin, when discussing the priorities in the defense industry, praised cyber weapons for their 'first strike' capability (Vasenin & Kuksin, 2013). Since then, a number of leader in the US national security as well as current US officials have been quoted comparing the threat caused by cyber weapons to nuclear weapons (Clapper, 2013).

Despite being more forward-leaning, the new strategy, even by promoting restraining operations in cyber space, still cannot ensure that such aggressiveness will not spill over to the rest of the warfighting domains or the international allies. Experts raise concerns that this new

cyber strategy will turn the internet into a Wild West of hacking operations (Groll, 2018). The concern intensifies as it is not clear how exactly the Trump administration will use the newly released offensive cyber strategy, as the policy's details remain classified and not available to the general public.

Earlier in this paper, the concept of mutually assured destruction was mentioned. But how does this concept apply to cyber space? Both the United States and Russia have claimed to have advanced cyber capabilities enough to remotely cause disturbances to each other's infrastructure. We are for once again at an impasse, where if one country attacks first, the other will like respond likewise. The concern rises when nations that have the motive, the expertise and the budget apart from the capabilities to conduct offensive cyber operations are simultaneously willing to establish the condition of mutually assured destruction. In this sense, they wish to avoid being outpaced in this initiative by their enemies. Clarke and Knake already anticipate nations preparing for conflict (Clarke and Knake 2013, p. 31). The ongoing nature of cyber war has been expressed through states hacking one another, causing disturbances to each other's networks and infrastructure, laying traps (ibid). One might wonder that this new dynamic might actually contribute towards maintaining the status quo and safeguarding peace and stability in cyber space. What if this offensive posture and alertness spirals out of control and further strain the diplomatic relations of nations in cyberspace?

This paper seeks to raise the issue of cyber deterrence, to rely on the possible scenarios that would follow a series of offensive operations in cyberspace, and to discuss their threat to the stability of the international system. This concern, however, does not entail solely offensive kinetic attacks. It has been frequently suggested that conflicts now could originate in the cyber domain and spillover from the digital realm to the international one (Kello, 2013). Simultaneously, the US willingness to act if attacked combined with its cyber capabilities logically leads to a more unstable world. A more assertive US posture could eventually have a cascading effect that would ultimately precipitate the security dilemma in the international system. Nobody could guarantee that this new reality could represent a whole new direction acquired by states in order to settle their disputes and to handle imminent threats. "The cyber domain is a perfect breeding ground for political disorder and strategic instability. Six factors contribute to instrumental instability: offense dominance, attribution difficulties, technological

volatility, poor strategic depth, and escalatory ambiguity" (Ibid, p.32). Hence, according to Kello, cyber conflict spillover into the conventional warfighting domains is not only possible but also inevitable.

A more offensive posture could be interpreted through counter intelligence gathering. Innocuous at first glance, as "[c]onsuming information about adversaries, tools or techniques and applying this to incoming data to identify malicious activity" could be considered valid for active defense standards (Bianco, 2014). Intelligence gathering can also be included in the strategic writing of a state with weaker capabilities. Pollpeter (2015) points out the inclination of China towards cyber espionage tactics in their effort to not be outpaced by their technologically advanced adversary. In their turn, the United states have been accused of launching such operations. This leads to the logical conclusion that such campaigns have already been normalized in the context of the diplomatic relations of these countries.

While cyber tools will likely integrate further into current war tactics and strategies, yet the concept of outright cyberwar is still rather speculative. For Kello, the fact that the world hasn't witnessed any serious cyber escalations, it does not mean that they will not occur in the future (2013, p.7). Clarke and Knake share the same perspective as well and anticipate the worst yet to come regarding cyber warfare (2010, p. 30-31). In addition, even the academic and political discourse is simply speculating whether or not a cyber arms race is even possible to occur.

The strategic bipolarity model that defined the Cold War era no longer represent the international system, especially in terms of physical conflict (Curtis, 2000). Researchers have been struggling to examine whether this could be an applicable model for cyberspace and information warfare. Even though this paper does not aim at providing answers over this debate, it cannot help but observe that the current situation in the world of conflict is a state of strategic multi-polarity, with multiple players and means of warfighting.

While we might find ourselves in a Cyber Cold War, there is one aspect of this part of our contemporary history that has not surfaced yet, the demonstration of capabilities. To be more specific, nobody can ever really forget the nuclear bomb that was dropped in 1945 on Hiroshima. The world is still recovering from its repercussions. When it comes to the cyber domain, such a

step has not been taken to demonstrate the possible consequences of a cyber attack. Indeed, there have been incidents where sophisticated attacks have caused disruptions in critical infrastructure or breaches in information systems, however, there has not been a recorded incident that was caused by an adversary with malicious intent. Hence, while the current state of great-power relations may resemble the Cold War era, I believe that the worst is yet to come. And this could change rapidly in the near future, same as political and international partnerships can deteriorate and technology develops as fast as a click of a mouse. Luckily the same technology that makes states vulnerable to potential cyber attacks, simultaneously, could be their chance to salvation.

As previously mentioned, the deployment of cyber weapons could result in numerous smaller scale attacks, the numbers of which are in fact growing dramatically, rather than in catastrophic attacks. Recent events in cyber history demonstrate that political actors are willing to use cyber weapons as a means of statecraft.[5]Looking ahead, although the odds are that the world will not experience a great scale cyber disaster, we cannot turn a blind eye towards the ever-growing number of smaller attacks we are already witnessing. While comparing and contrasting the analogy between cyber and nuclear weapons, the proliferation issue arises. That is, the supply and demand factors that affect the ability and willingness of different actors in their efforts to acquire the capability (Lindsay, 2019). More specifically, the international community has been very successful in preventing nuclear weapons from falling into the hands of reckless actors and regimes. This, however, is hardly the case in the cyber domain, where not only the proliferation but also the weaponization and employment of cyber tools can be observed.

It became clear that the US government considers that their financial and political interests, as well as their safety and sovereignty are better protected by taking a more proactive approach to cyber security. One approach to cyber security is active defense. The definition of active defense differs, ranging from using non-intrusive means, making the potential attacker doubt the success of their attack, to “hacking back”, meaning direct counter attacks. However,

[5] Rigorous Chinese espionage, Russian denial-of-service attacks in Estonia, Georgia and Ukraine, U.S.-Israeli sabotage of Iranian nuclear infrastructure, Russian hacking to the US presidential elections, the North Korean disturbance attack against Sony, etc.

this term still lacks a universally accepted definition. According to the Department of Defense Strategy for Operating in Cyberspace in 2011

> Active cyber defense is [the Department of Defense's (DoD's)] synchronized, real-time capability to discover, detect, analyze, and mitigate threats and vulnerabilities. It builds on traditional approaches to defending DoD networks and systems, supplementing best practices with new operating concepts. It operates at network speed by using sensors, software, and intelligence to detect and stop malicious activity before it can affect DoD networks and systems. As intrusions may not always be stopped at the network boundary, DoD will continue to operate and improve upon its advanced sensors to detect, discover, map, and mitigate malicious activity on DoD networks. (U.S. Department of Defense, 2011)

Taking a closer look into this definition, one might notice that despite being lengthy, it is not necessarily adequate. A threat can be mitigated in various ways; from re-enforcing antivirus and firewall to actually using kinetic force to physically cause disturbances to an enemy's infrastructure. As Christopher Jarko very well illustrates, "[online adversaries] exploit weaknesses and vulnerabilities in order to gain at the expense of or humiliate their victims. People who do this on the street are called bullies. There are many potential responses to a bully. One could submit to their demands, flee, respond with violence, or report the incident to the authorities. (p.20, Christopher Jarko, SANS institute) This paper will mainly focus on the latter option, that of the attack. As the name itself implies, an attack refers to causing adverse effects on an adversary's infrastructure.

Governments desiring to employ this method of defense should take into account that precise language is very important, whether as a result of a legal or political action or as a result of public disclosure. In that case, the intent to use (active) defense should be well documented in advance and the necessary actions should be taken in the spirit of transparency. This way the issued policy will be expressed through policy language that confirms the state's intent prior to the use of active defense and can also be made public.

7 Conclusion

This paper aimed at providing an overview of definitional and process issues that followed the changes in the Department of Defense's Cyber Strategy. The research has delineated and briefly discussed the different legitimations strategies of political discourse as introduced by Reyes. Along the way, various assumptions were discussed, among them the ability of offensive capabilities to deter further attacks in cyberspace; and the probability of increasing numbers of penetrations in cyberspace leading to further escalation of violence and insecurity among states.

Over the past 10 years, there has been an exponential increase in frequency and sophistication of attacks against US networks. As the possibility of cyberwarfare threats to US national security has become more prominent, the Pentagon has built robust defenses around military networks and the Department of Defense has made substantial efforts to integrate cyberdefence capabilities across military operations. Albeit a sizable amount of primary work remains, the US government has gradually stepped up by taking initiatives to defend the United States in cyberspace.

Networks and cyber tools serve the military more than any other previous developed technology by enhancing the defensive as well as the offensive capacity of states. Simultaneously, however, it makes them vulnerable to disruption and attacks in unprecedented and unanticipated ways. For this reason, the US government should assess whether or not the security gained by 'defending forward' is worth the potential risks, which would entail not only legal repercussions but also political as well as diplomatic risks. Undoubtedly, with the rising number of high-profile cyber attack incidents documented, it seems reasonable to believe that a state could benefit from some degree active defense. Given the dominance of offense in cyberspace, U.S. defenses need to be dynamic. As far as responsibility of the state, the US government is deploying all these defenses in a way that meets its obligation to protect the civil liberties of U.S. citizens. Currently, the US government posits that consistent use of counter attacks and the adoption of forward defense could serve to deter cyber attacks and urge that through the DoD strategy a new regime should be implemented to permit these strategies be a priority.

To sum up, we know yet very little about the potential impact of cyber activities and how cyber campaigns could be aligned with conventional tactics. Our core speculation refers to how cyber conflict will ultimately bleed into the other physical domains and affect the peace and stability in the international political system. For this reason, cyber policy and strategy should favor restraint over offense in protecting the digital realm. A policy of restraint that maintains control over cyber operations and does not suggest a more offensive stance is thus strategically wise. Concluding this thesis, the importance of language and rhetoric for appropriately framing and legitimizing cyber threats is clear. The evolution of cyber strategies proves that decision-makers and political leadership are slowly coming to this understanding as well. The analysis presented here could assist scholars and political authorities understand the emergence and importance of a conflict escalation and spillover in the digital commons through the Cold War analogy as a first step towards more appropriate strategies for cyber security threats.

Further questions

Taking this analysis into consideration, some interesting points for further discussion would be whether states that authorize a cyber operation against an adversary would risk the chance of retaliation throughout the warfighting domains. And how should leaders and decision makers look towards the wide-open future of cyber warfare? Following the existing literature and norms by comparing cyber weapons almost exclusively to nuclear weapons has led to a more restricted thinking. In contrast to a single weapons system, a better approach could be to trace back to the original principle that ties the two technologies together. That is, the core element of the nuclear-cyber analogy is that cyber weapons appear to revolutionize military and security affairs as nuclears did in the past.

This thesis has illustrated that a destructive conflict in cyberspace is feasible and that its consequences would be unbearable not only for the United States but for the rest of the world. Beyond any doubt, the US are called to find a solution. This solution could be defensive in nature, it could be also rather offensive. The US DoD has introduced a framework that would permit the use of active defense in cyberspace. As already discussed, this could include

technologies that, firstly, detect attacks; secondly, trace the attacks to their source; and enable counterattacks or simple intelligence-gathering practices.

Although the political leadership will decide what the execution threshold is and what the appropriate threat response will be, the US need to ensure their cyber capabilities. As such, not only need they be able to withstand an attack but also retaliate against a first strike by an adversary, whether it is a kinetic or a non-kinetic strike. What has been established so far with the new cyber strategy of the DoD is the US clearly articulating their willingness to respond to the threat. In this respect, it is of utmost important that any applied strategy must be communicated with great care and with a clear message. The message must also articulate what the execution threshold is and what the possible response will be. This is something that the new DoD policy certainly does not clarify.

References

Office of the President of the United States (2003). *The National Strategy to Secure Cyberspace*. Washington, D.C.

Krebs, B. (2005). A Short History of Computer Viruses and Attacks. *The Washington Post*, 14 Retrieved from: http://www.washingtonpost.com/wp-dyn/articles/A506362002Jun26.html

Ali, A. M., & Yusof, H. (2011). Quality in qualitative studies: The case of validity, reliability and generalizability. *Issues in Social and Environmental Accounting*, *5*(1/2), 25-64.

Altheide, D. L., & Johnson, J. M. (1994). Criteria for Assessing Interpretive Validity in Qualitative Research. In N. K. Denzin & Y. S. Lincoln (Eds.). Handbook of Qualitative Research, pp. 485-499. Thousand Oaks, CA: SAGE.

Arquilla, J., & Ronfeldt, D. (1993). Cyberwar is coming!. *Comparative Strategy*, *12*(2), 141-165.

Baxter, P., & Jack, S. (2008). Qualitative case study methodology: Study design and implementation for novice researchers. *The qualitative report*, *13*(4), 544-559.

Bayram, F. (2010). Ideology and political discourse: a critical discourse analysis of Erdogan's political speech. Annual Review of

Bello, U. (2013). " If I Could Make It, You Too Can Make It!" Personal Pronouns in Political Discourse: A CDA of President Jonathan's Presidential Declaration Speech. International Journal of English Linguistics, 3(6), 84.

Bendiek, A., & Metzger, T. (2015). Deterrence theory in the cyber-century. *INFORMATIK 2015*, 553–570

Blackmore, J. & Lauder, H. (2005). Researching policy. In B. Somekh and C. Lewin (Eds.) Research Methods in Social Sciences (pp. 97-104). Sage: London.

Bloomberg News (2013) Chinese General With Dempsey Compares Cyber-Attack to Nuke. *Bloomberg.* Retrieved from: https://www.bloomberg.com/news/articles/2013-04-22/china-seeks-to-forge-new-type-of-military-relationship-with-u-s-

Blumberg, B., Cooper, D. R., Schindler, P. S. (2005). Business research methods. Berkshire: McGrawHill Education.

Browne, J., Coffey, B., Cook, K. et al (2018). A guide to policy analysis as a research method. Health Promotion International 1-13. Oxford University Press. Doi: 10.1093/heapro/day052.

Buchanan, B. (2016). *The cybersecurity dilemma: Hacking, trust, and fear between nations*. Oxford University Press.

Carter, A. (2015). Drell Lecture: Rewiring the Pentagon: Charting a New Path on Innovation and Cybersecurity. Stanford, CA: Stanford University. Available at: defense.gov/DesktopModules/ArticleCS/Print.aspx?PortalId=1&ModuleId=2575&Article=606666, accessed August 24, 2016.

Cavelty, M. D. (2010). Cyberwar. In G. Kassimeris & J. Buckley (Eds.), *the Ashgate Research Companion to Modern Warfare* (pp. 123-144). Aldershot: Ashgate. p.127

Cavelty, M. D. (2013). Cyber security. In A. Collins (Ed.), *Contemporary Security Studies* (3 ed., pp. 361-378): OUP Oxford. P. 369

Cirenza, P. (2016). The flawed analogy between nuclear and cyber deterrence. *Bulletin of the Atomic Scientists*, *22*. Retrieved from: https://thebulletin.org/2016/02/the-flawed-analogy-between-nuclear-and-cyber-deterrence/

Clapper, J. R. (2013). Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community, Senate Select Committee on Intelligence, James R. Clapper, Director of National Intelligence, March 12, 2013. In *United States. Office of the Director of National Intelligence*. United States. Office of the Director of National Intelligence.

Clarke, R. A., & Knake, R. K. (2014). *Cyber war*. Old Saybrook: Tantor Media, Incorporated.

Curtis, W. (2000). The Assured Vulnerability Paradigm: Can it Provide a Useful Basis for Deterrence in a World of Strategic Multi-Polarity?. *Defense Analysis*, *16*(3), 239-256.

David Bianco, *Use of the Term "Intelligence" in the RSA 2014 Expo*, ENTERPRISE DETECTION & RESPONSE (Feb. 28, 2014) Retrieved from: http://detectrespond.blogspot.com/#!/2014/03/use-of-term-intelligence-at-rsa.html

Demchak, C. C., & Dombrowski, P. (2011). *Rise of a cybered westphalian age*. AIR UNIV MAXWELL AFB AL STRATEGIC STUDIES QUARTERLY.

Denning, D. E. (2015). Rethinking the Cyber Domain and Deterrence, *Joint Force Quarterly*

Denzin, N. K., & Lincoln, Y. S. (2005). Introduction: The Discipline and Practice of Qualitative Research. In N. K. Denzin & Y. S. Lincoln (Eds.), The Sage handbook of qualitative research (pp. 1-32). Thousand Oaks, CA, : Sage Publications Ltd.

Department of Defense. (2011). Joint Publication (JP) 1-02, Department of Defense Dictionary of Military and Associated Terms. p107. Retrieved from: http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf

Department of Defense. 2015. "The DOD Cyber Strategy". 17 April. Retrieved from: https://www.defense.gov/Portals/1/features/2015/0415_cyberstrategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

Dunmire, P. L. (2007). Emerging threats and coming dangers: Claiming the future for preventive war. In: Hodges A and Nilep C (eds) *Discourse, war and terrorism*. 19-43.

Education, Communication & Language Sciences, 7.

Eisenhart, C., & Johnstone, B. (2008). Discourse analysis and rhetorical studies. *Rhetoric in Detail: Discourse Analysis of Rhetorical Talk and Text. Amsterdam and Philadelphia: John Benjamins Publishing*, 3-21.

European Commission, High Representative of the Union. (2013). - JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Cyber Security Strategy of the European Union: An Open, Safe and

Secure Cyber space. I Final, 3. Retrieved from: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013JC0001&from=EN, 26 February 2018.

Fairclough, N. (2013). *Critical discourse analysis*. R. Wodak (Ed.). London: Sage.

Finlay, C. J. (2018). Just war, cyber war, and the concept of violence. *Philosophy & Technology*, *31*(3), 357-377.

Fischer, F. (2003). Reframing Public Policy: Discursive Politics and Deliberative Practices. Oxford: Oxford University Press.

Foucault, M (1972). *The Archaeology of Knowledge and the Discourse on language* (trans. Sheridan Smith AM). New York: Pantheon

Fung, B. (2013). "How Many Cyberattacks Hit the United States Last Year?" *Nextgov*. Retrieved from: http://www.nextgov.com/cybersecurity/2013/03

Geist, E. (2015). Deterrence Stability in the Cyber Age. *Strategic Studies Quarterly*, *9*(4).

Gilpin, R. (1981). *War and change in world politics*. Cambridge University Press.

Goldman, E. O., & Eliason, L. C. (2003). *The diffusion of military technology and ideas*. Stanford University Press.

Goodman, W. (2010). Cyber Deterrence: Tougher in Theory than in Practice? *Strategic Studies Quarterly* 4(3): 102– 35

Greenwald, G., & MacAskill, E. (2013). Obama orders US to draw up overseas target list for cyber-attacks. *The Guardian*, *7*. Retrieved from: https://www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas

Groll, E. (2018). Trump has a new weapon to cause 'the cyber' Mayhem. *Foreign Policy.* Retrieved from: https://foreignpolicy.com/2018/09/21/trump-has-a-new-weapon-to-cause-the-cyber-mayhem/

Herz, J. H. (1950). Idealist Internationalism and the Security Dilemma. pp. 157–180.

Herz, J. H. (2003). The security dilemma in international relations: background and present problems. International Relations, 17(4), 411-416.

Huth, P. K. (1999). Deterrence and international conflict: Empirical findings and theoretical debates. *Annual Review of Political Science*, *2*(1), 25-48.

Isnarti, R. (2016). A Comparison of Neorealism, Liberalism, and Constructivism in Analysing Cyber War. Andalas Journal of International Studies (AJIS), 5(2), 151-165.

Jalali, M. S. N., & Sadeghi, B. (2014). A critical discourse analysis of political speech of four candidates of Rasht City Council Elections in 2013, with a view to Fairclough approach. *European Journal of Social Science Education and Research*, *1*(2), 8-18.

Japan, "Cyber Security Strategy of Japan," June 2013, 41, http://www.nisc.go.jp/eng/pdf/

Jason Healey at SDA, Annual conference 2014, 31

Jervis, R. (1978). Cooperation under the security dilemma. *World politics*, *30*(2), 167-214.

Jervis, R. (1979). Deterrence theory revisited. *World Politics*, *31*(2), 289-324.

Jervis, R. (2017). Perception and Misperception in International Politics: New Edition. Princeton University Press.

Johnson, D. B. (2018) White House rolls out new national cyber strategy. *FCW.* Retrieved from: https://fcw.com/articles/2018/09/20/wh-cyber-policy.aspx

Joint Publication (JP) 1-02, (2010) *Department of Defense Dictionary of Military and Associated Terms*, 8 November 2010 (as amended through 31 January 2011) Retrieved from: http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf

Jon Lindsay, "CYBER OPERATIONS AND NUCLEAR WEAPONS", NAPSNet Special Reports, June 20, 2019, https://nautilus.org/napsnet/napsnet-special-reports/cyber-operations-and-nuclear-weapons/

Kello, L. (2013). The Meaning of the Cyber Revolution: Perils to Theory and Statecraft. *International Security* 38(2): 7– 40.

Kerry, J. (2013). Statement of Senator John F. Kerry, Nominee for Secretary of State. *Conformation Before the Senate Committee on Foreign Relations*. Retrieved from: https://www.govinfo.gov/content/pkg/CHRG-113shrg86451/pdf/CHRG-113shrg86451.pdf

Kollars, N., & Schenieder, J. (2018). Defending Forward: The 2018 Cyber Strategy is Here. *War on the Rocks September, 20.* Retrieved from: https://warontherocks.com/2018/09/defending-forward-the-2018-cyber-strategy-is-here/

Layne, C. (1993). The unipolar illusion: Why new great powers will rise. *International security*, *17*(4), 5-51.

Libicki, M. C. (2009). *Cyberdeterrence and cyberwar*. Rand Corporation. Retrieved from: https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf

Lindsay, J. R. (2013). Stuxnet and the limits of cyber warfare. *Security Studies*, *22*(3), 365-404.

Lonsdale, D. J. (2018). Warfighting for cyber deterrence: a strategic and moral imperative. *Philosophy & technology*, *31*(3), 409-429.

Louis, W. (2011). GCHQ: The Uncensored Story of Britain's Most Secret Intelligence Agency, by Richard J. Aldrich. *The English Historical Review*, *126*(520), 759-761

Lynn III, W. F. (2010). Defending a new domain-the Pentagon's cyberstrategy. Foreign Aff., 89, 97.

Mack, N. (2005). Qualitative research methods: A data collector's field guide.

Maness, R. C., & Valeriano, B. (2016). Cyber spillover conflicts: transitions from cyber conflict to conventional foreign policy disputes?. In *Conflict in Cyber Space* (pp. 61-80). Routledge.

Mearsheimer, J. J. (2001). *The Tragedy of Great Power Politics*. New York: Norton, "Anarchy and the Struggle for Power", Chapter 4

Morgan, P. M. (2010). Applicability of traditional deterrence concepts and theory to the cyber realm. In *Proceedings of a workshop on deterring cyberattacks: Informing strategies and developing options for US policy* (pp. 55-76).

Morgan, P. (2003). Deterrence Now. Cambridge: Cambridge University Press.
Morgenthau, H. J. (1948). *Politics among Nations: The Struggle for Power and Peace*. New York: Alfred A. Knopf.
Nakashima, E. (2018). White House authorizes 'offensive cyber operations' to deter foreign adversaries. *The Washington Post*, *20*. Retrieved from: https://www.washingtonpost.com/world/national-security/trump-authorizes-offensive-cyber-operations-to-deter-foreign-adversaries-bolton-says/2018/09/20/b5880578-bd0b-11e8-b7d2-0773aa1e33da_story.html
Nye, J. S. (2011). *Nuclear lessons for cyber security*. AIR UNIV PRESS MAXWELL AFB AL
Nye, J. S. (2011) The Future of Power. New York: PublicAffairs.
Owens, W., Dam, K., and Lin, H.(2009) Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities.Washington: National Academies Press. 294.
Pellerin, C. (2010). "Lynn: Cyberspace is the New Domain of Warfare". U.S. Department of Defense. Retrieved from: https://archive.defense.gov/news/newsarticle.aspx?id=61310
Permik. P., Wojtkowiak. J., Verschoor-Kirss. A. (2016). National Cyber Security Organisation: UNITED STATES. Tallinn: CCD COE Publication, 8.
Philbin, Lt. Col. Michael J. (2013). "Cyber Deterrence: An Old Concept in a New Domain." U.S. Army War College: Strategy Research Project.
Pijovic, N. (2016). "How Trump will test international relations theory. Will the realists or the constructivists be proved right?". Asia and the Pacific Policy Society. Retrieved from: https://www.policyforum.net/trump-will-test-international-relations-theory/
Pollpeter, K. (2015). Chinese writings on cyberwarfare and coercion. *China and cybersecurity: espionage, strategy, and politics in the digital domain*, 147.
Pomerleau, M. (2018) DoD releases first new cyber strategy in three years. *Fifth domain.* Retrieved from: https://www.fifthdomain.com/dod/2018/09/19/department-of-defense-unveils-new-cyber-strategy/
Pool, P. (2013). War of the cyber world: The law of cyber warfare. *Int'l Law.*, *47*, 299.
Quester, G. H. (2019). *Deterrence Before Hiroshima*. Routledge.
Rashid, F.Y. (2018). Understanding the Defense Department's New Cyber Strategy. *Desipher*. Retrieved from: https://duo.com/decipher/understanding-the-defense-departments-new-cyber-strategy
Reardon, R., & Choucri, N. (2012, April). The role of cyberspace in international relations: A view of the literature. In ISA Annual Convention, San Diego, CA (Vol. 1).
Reiter, B. (2017). Theory and methodology of exploratory social science research. *International Journal of Science and Research Methodology*, *5*(4).

Reyes, A. (2010). Power, emotions and agency in political discourse. In: Mantero M, Chamness Miller P and Watzke JL (eds) *Readings in Language Studies, Volume II: Language and Power*. Wilmington, DE: International Society for Language Studies, 201-218.

Reyes, A. (2011). Strategies of legitimization in political discourse: From words to actions. *Discourse & Society*, *22*(6), 781-807.

Rid, T. (2011). "Cyber War Will Not Take Place", Journal of Strategic Studies. Vol 35: p. 5-32

Rojo, L. M., & Van Dijk, T. A. (1997). "There was a Problem, and it was Solved!": Legitimating the Expulsion of Illegal 'Migrants in Spanish Parliamentary Discourse. *Discourse & Society*, *8*(4), 523-566.

Rudesill, D.S. (2018) Trump's Secret Order on Pulling the Cyber Trigger. *Lawfare blog.* Retrieved from: https://www.lawfareblog.com/trumps-secret-order-pulling-cyber-trigger

Serbu, J. (2018). DoD, DHS reach accord on new steps to cooperate in cyber defense. *Federal news network.* Retrieved from: https://federalnewsnetwork.com/cybersecurity/2018/11/dod-dhs-reach-accord-on-new-steps-to-cooperate-in-cyber-defense/

Shackelford, S. J. (2009). From nuclear war to net war: analogizing cyber attacks in international law. *Berkeley J. Int'l Law*, *27*, 192.

Singh, A. S. (2014). Conducting Case Study Research in Non-Profit Organisations. Qualitative Market Research: An International Journal, 17, 77–84.

Smeets, M. (2018). The Strategic Promise of Offensive Cyber Operations. *Strategic Studies Quarterly*, *12*(3), 90-113.

Stolberg, A. G. (2013). *How Nation-States Craft National Security Strategy Documents (Enlarged Edition)*. Lulu. com. 73.

Strauss, S., & Feiz, P. (2014). Discourse analysis; Putting Our Worlds into worlds (1st ed.). New York, NY: Routledge.

Swift, J. (2009). The Soviet-American Arms Race. *History Review*, (63), 13.

THE DEPARTMENT OF DEFENSE CYBER STRATEGY. (2015), 4-27. Retrieved from: https://www.defense.gov/Portals/1/features/2015/0415_cyberstrategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf, 22 March 2018

Thucydides. *History of the Peloponnesian War*, trans. Rex Warner, Harmondsworth: Penguin Books, 1972.

United States. (2017). *The national security strategy of the United States of America*. Washington: President of the U.S.

Unknown (2009) South Korea to set up cyber command against North Korea – two years earlier than planned. *Channel News Asia*

Valeriano, B., & Maness, R. C. (2015). *Cyber war versus cyber realities: Cyber conflict in the international system*. Oxford University Press, USA.

Van Dijk, T. A. (2003). The discourse-knowledge interface. In *Critical discourse analysis* (pp. 85-109). Palgrave Macmillan, London.

Van Dijk, T. A. (2005). Politics, ideology and discourse. In: Ruth Wodak, (Ed.), Elsevier Encyclopedia of Language and Linguistics. Volume on Politics and Language, 728-740.

Van Leeuwen, T (2007). Legitimation in discourse and communication. *Discourse & Communication* 1(1): 91-112

Van Leeuwen, T., & Wodak, R. (1999). Legitimizing immigration control: A discourse-historical analysis. *Discourse studies*, *1*(1), 83-118.

Vasenin V.,& Kuksin S. (2013) The text of the speech of Dmitry Rogozin at a press conference in the RG. Original (in Russian) Retrieved from: https://rg.ru/2013/06/28/doklad.html

Vasquez, John A. 1995. *Classics of International Relations.* Pearson. 9-19

Waltz, K. (1979). Theory of international politics. Reading, Mass.: Addison-Wesley Pub. Co

White House Fact Sheets. (2018). President Donald J. Trump is Strengthening America's cybersecurity. Retrieved from: https://www.whitehouse.gov/briefings-statements/president-donald-j-trump-is-strengthening-americas-cybersecurity/

White House. (2018) President Trump Unveils America's First Cybersecurity Strategy in 15 Years. The White House.

Wodak, R. (2001). What CDA is about-A summary of its history, important concepts and its developments, in methods of Critical Analysis. In Ruth Wodak and Micheal Meyer (Ed), SAGE Publications, India Pvt Ltd.

Zakaria, F. (1999). *From wealth to power: The unusual origins of America's world role* (Vol. 82). Princeton University Press.

Zheng, D. (2015). DOD Cyber Strategy'. *Center for Strategic & International Studies*. Retrieved from: https://www.csis.org/analysis/2015-dod-cyber-strategy