Fake News! An Analysis on which Factors shaped the US Attitude towards Russian Disinformation in the Cold War and the Information Age

Floor Wierenga

Master Thesis Crisis and Security Management

Dr. C.W. Hijzen

Dr. S.D. Willmetts

January 10, 2021

Wordcount: 23.929 words – Excluding bibliography

Universiteit Leiden
Campus Den Haag

Table of Content

1. Introduction

The presence of fake news is everywhere, both off and online, and for its recipients it is hard to separate the fake from the real news. The term 'fake news' may have become more popular in use since Donald Trump, but the phenomena is far from new. Fake news has been around for centuries and is also known as disinformation. Disinformation campaigns can be traced back as far as the Roman period. In 44BC, the decision from Julius Caesar to declare himself ruler for life was met with some resistance from a group called 'the liberators' led by Brutus (Kaminska 2017). What followed was a disinformation war, using various tactics to confuse and destabilize the opposition (Kaminska 2017). This thesis will examine cases of disinformation in the Cold War and the information age in order to identify differences and similarities that will contribute to a better understanding of disinformation and on how it could be countered.

1.1. What is Disinformation?

Disinformation is defined as "The dissemination of deliberately false information, esp. when supplied by a government or its agent to a foreign power or to the media, with the intention of influencing the policies or opinions of those who receive it." (Cheyfitz 2017, 15) As stated by Prof. Dr. A. Gerrits, a professor in global politics, in his article on disinformation in international relations, disinformation is not a new phenomenon, it has been a part of warfare and foreign policy for many ages (2018, 5). Many nations have weaponized information in order to gain an advantage over their adversaries, hence, many nations have been the target of such information attacks. Disinformation is widely regarded to be a threat to democracy, partly due to its political polarizing effects (Gerrits 2018, 6). It also has the ability to influence the behavior of the target which makes it a powerful tool in both conflict and international politics (Lanoszka 2019, 7).

1.2. Problem Description

Disinformation is becoming an increasingly complex threat, now involving all aspects of society and used not only by state, but also non-state actors (Gerrits 2018, 22). As stated by Thomas Rid, expert in the field of risks of information technology in conflict, it is important to look at the historical cases of disinformation if one wants to fully understand the concept of disinformation and its future consequences (Rid 2020, 14). He goes on to state that "Ignoring the rich and disturbing lessons of industrial-scale Cold War disinformation

campaigns risks repeating mid-century errors that are already weakening liberal democracy in the digital age." (Rid 2020, 16) During the Cold War, the Soviet Union ran several disinformation campaigns. One of the most famous being operation InfeKtion (1980s), which was centered around convincing the world that the HIV/AIDS virus was designed and developed in a lab in the US with the intent of being used as a biological weapon (Rid 2020, 15). This campaign will be used as a case study. More recently, Russia has been accused of spreading disinformation in order to destabilize the conflict in Eastern Ukraine and meddling in American presidential elections, all to sway local politics in their favor. However, Russia is not the only nation involved in disinformation campaigns. In 2019, Facebook and Twitter revealed that they took down close to a 1000 accounts that were involved in the delegitimization of the pro-democracy movement in Hong Kong (Banjo 2019). They also revealed that these accounts were part of a larger disinformation campaign backed by the Chinese government. On more than one occasion these messages led to violence, showcasing the dangers involved with spreading disinformation.

1.2.1. Aim of this Research

One of the main concepts tied to disinformation is the concept of truth. It has been said that nowadays we are living in a "a post-truth era—an era in which audiences are more likely to believe information that appeals to emotions or existing personal beliefs, as opposed to seeking and readily accepting information regarded as factual or objective." (Cooke 2017, 212) This leads one to questions whether or not one can still speak of a concept such as the 'truth'. The 'truth' seems to be what people make of it with help of their feelings and already existing notions. This makes the 'truth' easy to manipulate by others playing into these feelings and notions. Can a manipulated 'truth', especially when widely believed, still be called truth? Or should a manipulated truth be seen as misinformation or even disinformation? It is questions like these that lie at the foundation of the disinformation problem. When one decides to see manipulated truth as disinformation it is important to fully understand this concept and its consequences. Fully understanding disinformation can lead to being able to detect it in earlier stages, identifying a way to counter it and being able to get closer to the factual truth. This thesis aims to aid in this process by looking at historical cases of disinformation. Misinformation will be briefly defined but is not part of the analysis performed in this thesis. In order to guide this research, the following research question will be applied: "*What factors shaped the United States' attitude towards Russian disinformation during Operation InfeKtion (1980s) and the Russian influence campaign in the United States*

in 2016 and how can the differences and similarities between these time periods be explained?" The added value of this research lies in the fact that this thesis historicizes the main questions in the disinformation literature, how does one identify disinformation and how does one counter it? It does not aim to find the 'right' answer to these two questions, instead it tries to understand how over time the US has developed different and transforming threat perceptions as well as counter strategies in regard to disinformation.

1.3. Case selection

This thesis will focus on two cases, namely, the Cold War case of Operation InfeKtion (1980s) and the more recent case of the 2016 presidential elections in the US. Operation InfeKtion was a Soviet campaign set up in 1985 as part of the Soviet Union's active measures during the Cold War (United States Department of State 1987, 33). The case of the 2016 presidential elections revolves around an elaborate campaign to discredit Clinton and support the candidate the Russians deemed more favorable to Russian objectives, Donald Trump (Walton 2019, 107) Both cases will be analyzed from the American perspective. This research has chosen to focus on Russian disinformation against the US due to various reasons. One of these reasons is that during both time periods there are rising tensions between these nations that seem to be accompanied by a heightened interest in disinformation campaigns. These two cases were partly chosen because of the fact that they are among the most well-known disinformation cases. More justifications will be discussed in chapter 3.2. In the case of the Cold War this thesis deals with the Soviet Union, which ceased to exist in 1991. Therefore, this thesis will refer to the nation as Russia, unless explicitly referring to it in the Cold War.

1.4. Analysis

The answer to the main research question will be given through analyzing mostly US government documents such as the official report on active measures in 1986-1987, congressional records as well as the official reports on the 2016 Russian influence campaign. These documents will be further elaborated upon in section 3.3. The documents will be analyzed through the lens of securitization theory. In this thesis, securitization will be defined as "an articulated assemblage of practices whereby heuristic artefacts (metaphors, policy tools, image repertoires, analogies, stereotypes, emotions, etc.) are contextually mobilised by a securitizing actor, who works to prompt an audience to build a coherent network of implications (feelings, sensations, thoughts, and intuitions) about the critical vulnerability of a referent object, that concurs with the securitizing actor's reasons for choices and actions, by

investing the referent subject with such an aura of unprecedented threatening complexion that a customised policy must be immediately undertaken to block it." (Balzacq, Léonard, and Ruzicka 2016, 495) The core concepts of securitization theory which this thesis will use are the 'securitizing actor', 'referent subject' and 'referent object'. The securitizing actor is "the agent who presents an issue as a threat through a securitizing move" (Balzacq, Léonard, and Ruzicka 2016, 495), the referent subject can be defined as the presence that is threatening, and the referent object is that what is being threatened. This thesis will use securitization theory to specify "how, and under which conditions, the security-ness of an issue is fixed." (Balzacq, Léonard, and Ruzicka 2016, 517) In this case, the issue is disinformation. In doing so, this thesis hopes to bring to light the attitude shaping factors and their influence on the extent to which disinformation was perceived and acted against as a threat to national security. Securitization theory will be discussed more extensively in chapter 3.

In practice this means that the documents will be looked at the following way. The securitization lens provides the opportunity to see why and how disinformation is perceived as a security threat. Looking for ways used by the securitizing actors to convince the audience that disinformation is a security threat that requires extraordinary measures. Researching problem perception in both time periods will identify factors that shaped the attitude of the US towards disinformation. Once these factors are compared, and both differences and similarities are identified, they could provide a valuable insight into the question of how to identify disinformation. The documents will also be analyzed to see what shaping factors can be identified with regards to counter measures which could, in combination with the problem perception research, lead to valuable insights into the other main question in disinformation literature on how to counter it. The main argument developed throughout the analysis is that historians have limited influence on the main questions surrounding disinformation since the question are looked at through a policy-oriented lens instead of a history-oriented one.

1.5. Relevance

The relevance of this research can be found in both the social as well as the academic field. The academic relevance of this research is that it combines several fields literature, such as Cold War literature, securitization literature, and intelligence studies literature, which the academic field has been previously lacking. As for the social relevance, disinformation is increasingly affecting daily lives. Disinformation has the tendency to exploit existing tensions and amplify them, for example racial tensions in the US. Due the internet, disinformation is easily spread and has therefore become more dangerous. It has been said that disinformation

weakens the liberal democracy due to the fact that disinformation diminishes the trust of the people in democratic institutions (Bennett and Livingston 2018, 127). This means that with every piece of disinformation an increasing number of people are turning against democratic institutions which can cause dangerous situations.

1.6. Structure

The next chapter of this thesis provides the body of knowledge fundamental to of this research. This chapter will highlight all the important fields of literature related to this research, such as Cold War literature, disinformation literature and intelligence literature, as well as introduce and define the important concepts. After that, a chapter will explain the methods applied in this research as well as provide justifications for the case studies and chosen documents. The chapters that follow will contain the analysis that will provide an answer to the research question. The first analytical chapter will analyze the documents based on problem perception. The second analytical chapter will do the same for counter measures. In the third analytical chapter the findings of the previous two chapters will be compared in order to identify differences and similarities. This chapter will also contain a policy recommendation. This thesis will end with a concluding chapter in which an answer to the research question as well as avenues for further research will be provided.

2. Body of Knowledge

This chapter will first provide a literature review to situate this research within the relevant, existing fields of literature. Afterwards, a comprehensive definition will be provided of the concepts that are central to this research such as disinformation, national security, Cold War, active measures and others.

2.1. Critical Literature Review

2.1.1. Introduction into disinformation

'Disinformation' is a word that can be traced back to the Cold War and is derived from the Russian 'dezinformatsiya' (Garthoff 2004, 51). As stated in the introduction, disinformation can be traced back as far as 44BC, to Caesar's declaration (Kaminska 2017). This declaration was met with resistance led by Brutus and resulted in the death of Caesar himself. The untimely demise of the general did not lead to the re-establishment of a republican system like Brutus had hoped. Rather it caused a power struggle between Octavian and Mark Anthony (Kaminska 2017). In order to win this power struggle, Octavian started a smear campaign against Mark Anthony (Kaminska 2017; Posetti and Matthews 2018), which Mark Anthony tried to discredit using his own propagandic materials but in the end he failed to do (Scott 1929, 141). Octavian started to spread pieces of information that suggested that Mark Anthony had given up his connection with their Roman ancestry for a barbaric woman, Cleopatra (Scott 1929, 136). Octavian spread his disinformation through speeches in the senate or by addressing his troops (Scott 1929, 136), he even went as far to make coins that featured both Mark Anthony and Cleopatra in order to get people to believe his claims (MacDonald 2017).

Further back in history, in the 5th century BC, Sun Tzu wrote his book 'The Art of War' (The Project Gutenberg eBook 2005, 2). In his book Sun Tzu stated that "All warfare is based on deception." (Tzu and Giles 1994, 24) Disinformation is a large part of the practice of deception. Much later, around the year 1450, Johannes Gutenberg invented a machine that would allow for a much easier large-scale spread of disinformation, the printing press (Taylor 2003, 88). The printing press facilitated the communication of, among other things, disinformation to a wider audience.

In the years that followed, disinformation was present in almost every conflict, however, it was often labeled as propaganda. It was not until the Cold War that scholars

widely started to refer to employing deliberately false information to harm your opponent as disinformation. Disinformation during Cold War times was one of the key offences employed by the Soviet Union against the West (Walton 2019, 110). The literature surrounding disinformation is a growing field (Bennett and Livingston 2018, 134). According to Calder Walton, "disinformation can be most usefully understood as a carefully constructed false message linked to an opponent's communication system to deceive its decision-making elite or public." (Walton 2019, 110) Cheyfitz defines disinformation as "The dissemination of deliberately false information, esp. when supplied by a government or its agent to a foreign power or to the media, with the intention of influencing the policies or opinions of those who receive it." (Cheyfitz 2017, 15) Both of these understandings of disinformation, as well as most of the other definitions available in the literature surrounding disinformation, have in common that they all highlight the deliberate nature of disinformation and its intention to cause harm. This is where disinformation differs from the concept of misinformation. These concepts are sometimes used synonymously, however, they are two distinct concepts in the eyes of intelligence professionals. Walton states "misinformation is false information that a government officially and openly disseminates, whereas disinformation is false information that is covertly disseminated—with no fingerprints of the state attached to it." (Walton 2019, 110) According to Hendricks and Vestergaard, when you are misinformed "you have factually false convictions that you believe to be true. Misinformation misleads citizens, politicians, and journalists. One may misinform others unintentionally by passing on information that is believed to be true, but which turns out to be false." (Hendricks and Vestergaard 2019, 54) Misinformation, however, turns into disinformation when the intention behind the information sharing is to harm (Hendricks and Vestergaard 2019, 54).

Not all scholars believe disinformation to be a threat of the highest priority. In his article on disinformation, Prof. Dr. Gerrits, takes a wide approach and aims to determine how important disinformation is to international relations. He emphasizes that in order to completely understand the extent of the disinformation threat one must do more than just look at history (Gerrits 2018, 19). It is a security issue that adapts and develops over time while having both international and domestic effects (Gerrits 2018, 19). According to Gerrits, disinformation is "at most a soft security challenge" (Gerrits 2018, 20) partly because he believes one cannot fully assess the effects of disinformation due to a lack of insight into the intentions behind it as well as the unwillingness of actors to admit they have been involved (Gerrits 2018, 20, 22). W. Lance Bennett and Steven Livingston, experts in the field of political science and international affairs, on the other hand view disinformation to be a more

dangerous threat than Gerrits does. They emphasize the effects that disinformation has on democracy, stating that it breaks down trust in democratic institutions (Bennett and Livingston 2018, 127). Marzena Araźna, an expert in international security, also highlights the seriousness of the disinformation threat by portraying it as a part of multidimensional warfare. The article emphasizes the shift in warfare tactics from armed conflict to warfare through information, of which disinformation is a large part (Araźna 2015, 126). The article also touches upon the shift in actors from state to non-state (Araźna 2015, 127), a recurring interest throughout the disinformation literature. Meaning that disinformation on a global level is no longer largely used by state actors but also by non-state actors such as companies or even individuals.

One of the most cited authors on disinformation and active measures is Ladislav Bittman, a former Czech-Slovakian deputy director of disinformation during the Cold War who defected to the US in 1968 where he became a professor in disinformation (Matz 2016, 171). When dealing with disinformation it is hard to assess the opponents' intentions. Garthoff writes, "Deception operations are carefully designed and conducted covert intelligence operations to mislead the adversary. They are, and will probably remain, one of the least disclosed areas of intelligence activity." (Garthoff 2004, 52) With his book "The KGB and Disinformation: An Insider's View", Bittman provides a unique insight into Soviet intentions behind disinformation as well as its operational structure during the Cold War. The first important thing highlighted by Bittman is that in order for disinformation to be successful, "every disinformation message must at least partially correspond to reality or generally accepted views." (Bittman 1985, 49) Bittman also writes that in the disinformation process "participants play one of three roles, where operator refers to the author behind the disinformation, adversary to a foreign state, and unwitting agent to 'a gameplayer who is unaware of his true role and is exploited by the operator as a means of attacking the adversary'."(Bittman 1985, 50-52; Matz 2016, 157)

2.1.2 Disinformation and the Field of Intelligence

One of the main fields of literature concerned with disinformation is intelligence studies. In intelligence theory, a highly relevant topic is 'denial & deception' since it is an undeniable fact for intelligence analysts dealing with intelligence objects of high interests (Bruce and Bennett 2014, 197). James Bruce and Michael Bennett, a former intelligence analyst and an expert on denial and deception, define denial and deception as any undertaking

(activity or program) by adversaries—state and nonstate actors alike—to influence or deceive policymaking and intelligence communities by reducing collection effectiveness, manipulating information, or otherwise attempting to manage perceptions of intelligence producers and consumers (for example, policymakers and warfighters) (Bruce and Bennett 2014, 197). They specify this definition by stating that the term deception "refers to manipulation of intelligence collection, analysis, or public opinion by introducing false, misleading, or even true but tailored information into intelligence channels with the intent of manipulating the perceptions of policymakers in order to influence their actions and decisions. The goal is to influence judgments made by intelligence producers and thus the consumers of their products." (Bruce and Bennett 2014, 198) Comparing the earlier presented definitions of disinformation to that of deception one could easily see why intelligence scholars view disinformation as a tool of deception (Smith 2014, 554).

Disinformation campaigns were not always executed by intelligence agencies. According to Rid, it was not until the second wave of disinformation that disinformation became professionalized (Rid 2020, 13). This second wave of disinformation, which started after World War II, saw American intelligence agencies leading the way in professional disinformation campaigns (Rid 2020, 13). At that time, the CIA preferred to call their operations 'political warfare' while Russia preferred the term disinformation. Both terms, however, had the same goal: "to exacerbate existing tensions and contradictions within the adversary's body politic, by leveraging facts, fakes, and ideally a disorienting mix of both." (Rid 2020, 13) This second wave of disinformation is part of what is known as the modern era of disinformation which is characterized by its four waves in which disinformation practices grew and evolved (Rid 2020, 13). The first wave started during the Great Depression in the interwar years. Influence operations during this time "were a weapon of the weak" (Rid 2020, 13) and at the time were nameless. The third wave started around the late 1970s. At this time, disinformation became a well-resourced, globally used weapon (Rid 2020, 14). The fourth wave of disinformation slowly became visible in the 2010s. This wave of disinformation is characterized by the fact that "the old art of slow-moving, highly skilled, close-range, labor-intensive psychological had turned high-tempo, low-skilled, remote, and disjointed." (Rid 2020, 14) This change was brought on by technological advancements and internet culture.

From the time disinformation became a professionalized tool, several agencies and departments have been tasked with managing it in the US as well as the Soviet Union. In this post World War II time period, the KGB in the Soviet bloc was tasked with disinformation operations. As stated by Bittman, a section of the KGB, known as the First Main Directorate,

was in control of covert operations and foreign intelligence (Bittman 1985, 18). In 1970, the KGB advanced their disinformation practices by giving it the rank of 'special section' which was named Service A (Bittman 1985, 39). Service A was in charge of preparing disinformation campaigns according to a long-term plan, usually between five to seven years (Bittman 1985, 45). Nowadays, the Russian disinformation system consists of more than just intelligence agencies. It is made up of several interconnected actors such as intelligence agencies, media outlets controlled by the state, accounts on social media and cyber criminals such as hackers (Nemr and Gangware 2019, 16).

Alongside the KGB operations coming from the Soviet Union, the US had their own disinformation campaigns coming from the CIA. Within the CIA the Office of Special Projects was created "to coordinate secret offensive operations against the expanding communist power." (Rid 2020, 77) This was shortly thereafter renamed to the Office of Policy Coordination presumably in order to draw attention away from their covert activities. A few decades later, in 1981, it was William Casey, who was brought on by President Reagan to become the Director of Central Intelligence, who pushed the intelligence community to pay more attention to Soviet Active Measures (Schoen and Lamb 2012, 26-27). In the same year the Active Measures Working Group (AMWG) was created (Schoen and Lamb 2012, 32). The AMWG was an interagency group that worked out of the State Department, later the United States Information Agency (USIA), to explicitly deal with Soviet disinformation practices (Schoen and Lamb 2012, 8). The AMWG was not classified but not very well-known (Ellick and Westbrook, n.d.). They were a group of part time intelligence professionals that received no government funding for their work.

After the Cold War had ended, many believed that the disinformation threat had ended with it (Jones 2018, 1). However, this was not the case. The Soviet Union may have disintegrated in 1991 but Russia did not stop their disinformation practices (Ellick and Westbrook, n.d.). The Russians kept producing disinformation, although on a smaller scale, while the US moved on to other threats. More recently, the Department of Homeland Security (DHS) got involved in the disinformation game. The DHS officially got involved in countering Russian disinformation in 2018 (Bodine-Baron et al. 2018, 14). As of today, the DHS, however, does not actively get involved in countering disinformation. Instead they have been focusing on the coordination of "information-sharing and partnerships between state and local governments, private sector companies, and federal departments and agencies." (Bodine-Baron et al. 2018, 14) The Department of Justice has been focusing on the legal aspects of countering disinformation (Bodine-Baron et al. 2018, 15). The US has also taken

counter measures through their legislation. For example, the National Defense Authorization Act (NDAA) (Bodine-Baron et al. 2018, 16).

2.1.3 Disinformation and the Cold War

When the Cold War started, the US had only just finished fighting the Second World War. The US had no desire to take part in a new war, however, they had even less desire to live in insecurity (Gaddis 2000, 353). At the end of the Second World War, the US gained a new responsibility due to their new-found power position. The responsibility to uphold their newly created world order which was compatible with their own values (Beisner, 2006, 642). The international order entered a new bipolar system which was characterized by a power struggle between the US and the Soviet Union (McMahon, 2009, 1). The fall of Nazi Germany caused a state of disarray in Europe, which created an opportunity for the US and the Soviet Union to spread their ideologies and values which led to a power struggle. This power struggle with the Soviet Union became the main motivator behind American foreign affairs and is now known as the Cold War (Jeansonne & Luhrssen, 2014, 82).

One of the most notable characteristics of the Cold War is the considerable use of propaganda. Propaganda has been existent throughout human evolution (Tutui 2017, 112). During the Cold War, the US used propaganda to spread their own ideas and values as did the Soviet Union. From the start of the Cold War, the Soviet Union organized a series of coordinated propagandistic attacks aimed at harming the US (Whitton 1951, 151). The Soviet Union used every tool of communication available to them for these attacks on the US, its policies and its leaders (Whitton 1951, 151). Both parties often used print media to spread their propaganda, for example through the use of comic books. Comics turned in to a way to translate the frontpages of the newspapers to a form that was easier understood by the public (Brunner 2010, 170). Newspapers themselves were an important way in which propaganda was spread. Almost all larger newspapers had a so-called ‘funnies page’, which was read by almost everybody in society (Brunner 2010, 171). On this ‘funnies page’ one would find a comic, which allowed the reader to take their own time to understand its message, whereas other media, such as film or radio, delivered these messages in such a way that they needed to be understood immediately since people are unable to inspect them at their own pace (Brunner 2010, 171). Radio, television and film on the other hand, were a great way to reach a wider geographical audience. It is important to note that at the start of the Cold War a television in the household was a rarity, but this changed rapidly as time passed (TVB 2019).

Another characteristic of the Cold War is the use of disinformation. Studies dealing specifically with how the Soviet Union conducted their disinformation operations are very rare (Matz 2016, 155) due to disinformation being a covert action. Disinformation in the Cold War days was part of what the Soviets called the art of combination (Kaplan 2019, 2). Nowadays, this is known as hybrid warfare. Hybrid warfare is defined as "a conflict where actors blend techniques, capabilities and resources to achieve their objectives." (Batyuk 2017, 464) Hybrid warfare is a concept characterized by its complexity due to "globalization, proliferation of weapons, advanced technology, transnational extremist activities and resurgent powers" and its property to combine old and new warfare tools and techniques (Araźna 2015, 115-116).

Many authors in the field of Cold War disinformation base their research on one of two questions. How do we identify disinformation and how do we counter it? In her article, Megan Reiss, an expert in national security issues, states there is a pressing need to find a way with which disinformation campaigns can be easily detected. According to Reiss, being able to identify disinformation campaigns in their early stages may prove to be a very effective countermeasure (Reiss 2019, 7). This statement shows both the importance and the interconnectedness of the two previously posed questions that surround disinformation literature. Reiss also states that in order to help answer these two overarching questions it is important to realize that a historical comparison on disinformation cases needs to be made (Reiss 2019, 1). In his report, Andersson, member of the Strategy and Policy Unit of the European Defence Agency (EDA), looks at the Cold War to gain a better understanding on how to counter disinformation. He emphasizes the importance of having a critical mind when it comes to assessing the truthfulness of information (Andersson 2015, 4). Andersson believes that teaching to have a critical mind in schools leads to a higher number of the population being 'immunized' against disinformation, which in turn will protect those that do not yet have a critical mindset. Johan Matz, an expert in political science, argues for a comparison of disinformation practices over time. He states that comparing cases of disinformation over time might reveal patterns which could prove useful in the disinformation identification process (Matz 2016, 157).

Cold War disinformation was part of 'active measures'. Thomas Rid states that it is of high importance to define what active measures is and what it is not because they are difficult to identify (Rid 2020, 16). First, active measures are methodically planned by large bureaucracies and not just unplanned lies made up by politicians. Second, an element of disinformation is present in all active measures. "Content may be forged, sourcing doctored,

the method of acquisition covert; influence agents and cutouts may pretend to be something they are not, and online accounts involved in the surfacing or amplifications of an operation may be inauthentic." (Rid 2020, 16) Third, active measures always have a goal which usually revolves around weakening the target (Rid 2020, 16). In short, "Active measures-such as the use of front groups or the spread of disinformation (lies)--are deceptive operations that attempt to manipulate the opinions and/or actions of individuals, publics, or governments." (United States Department of State 1987, iii)

2.1.4 Disinformation and the Information Age

Today we live in what is known as the information age. This age is characterized by its rapid developments of information technology which increasingly affects our daily life (Soma, Termeer, and Opdam 2016, 89). The information age influences "our social relationships (Twitter, Facebook and WhatsApp), our economy (virtual auction), our science (scientific information losing much of its credibility and authority due to a variety of other information sources), and our politics (WikiLeaks)." (Soma, Termeer, and Opdam 2016, 89) In other words, the information age describes a time in which many aspects of our daily lives are changing as a result of information production. "It is a shift from production-oriented to service-based occupations, the manipulation of symbols, and a decrease in the percentage of the labour force involved in the production of tangible products. Most importantly, society is characterized by the emergence of 'networked individualism' in which the likelihood of connectivity beyond the local group increases drastically." (Mesch and Talmud 2010, 2)

One major difference between Cold War disinformation and disinformation during the Information Age is technology. Research has shown that "technological development in the information sphere and global economic interdependency have fundamentally changed the societal and political context in which Active Measures are carried out." (Pynnöniemi 2019, 163) In august of 2020, the Global Engagement Center of the United States Department of State released a report in which they identify what they see as the pillars of Russia's disinformation and propaganda ecosystem (Global Engagement Center 2020, 1). Most of these pillars depend on modern day technology. The pillars as named in the report are official government communications, state funded global messaging, cultivation of proxy sources, weaponization of social media, and cyber-enabled disinformation (Global Engagement Center 2020, 8).

Nowadays, researchers tend to focus on the effect disinformation has on democracy. Hendricks and Vestergaard state that "Disinformation contributes to conflict, polarization, and

spiteful feelings potentially threatening to civilized and constructive political debate and social cohesion." (Hendricks and Vestergaard 2019, 69) They further emphasize the serious effects of disinformation on democracy by citing a survey conducted in the USA which stated that the fake news stream surrounding the 2016 presidential elections caused many respondents (63%) to be very confused (Hendricks and Vestergaard 2019, 70). They conclude that when disinformation reaches this extent it should most definitely be regarded as a threat to both democracy and security (Hendricks and Vestergaard 2019, 70). In the literature surrounding disinformation in the Information Age, researchers once again call for critical thinking. They state that we are living in what is known as "a post-truth era—an era in which audiences are more likely to believe information that appeals to emotions or existing personal beliefs, as opposed to seeking and readily accepting information regarded as factual or objective." (Cooke 2017, 212) This statement shows that we live in an age in which many are vulnerable to fall for disinformation. This vulnerability paired with new technology and the renewed emphasis of the threatening nature of disinformation shows the need for an answer to those two central questions, how do we identify disinformation and how do we counter it? Because only when there is an answer to those questions, can one properly defend against this growing threat.

2.1.5 Conclusion

To conclude this literature review, one can state that there is a need for more research on the subject of disinformation. Not because it has not been researched before, but because it remains an ever-changing threat which is not easily detected and countered. The first part of this literature review looked at the literature surrounding disinformation in general. The literature showed that disinformation is not a new phenomenon and has been around for centuries. It also showed that within disinformation literature there are several definitions, however, they all agree on the fact that disinformation is spread with the intention to cause harm. The second section dealt with disinformation as part of the intelligence sector. Disinformation has been part of the professionalized intelligence community since the second wave of disinformation. Both the US and Russia have had agencies that dealt with disinformation campaigns. In recent years, responsibility for countering disinformation in the US lies with the DHS. The third section focused on disinformation in the Cold War. The Cold War years are considered the prime years of active measures and disinformation. In the final section disinformation in the information age was discussed. During the information age,

there has been a huge change in the way that disinformation campaigns are conducted. Due to technological advancements disinformation is more easily created and spread, which makes it more dangerous.

The literature seems to be lacking a view of disinformation that combines multiple fields of study. This thesis aims to contribute to the disinformation literature by combining the previously discussed fields of research, Cold War literature, intelligence literature, information age literature, as well as securitization literature which will be elaborated on in the following chapter. The combination of these fields of literature is necessary in order to better understand an issue as complex as disinformation. This thesis will compare two cases of Russian disinformation against the US, selected from the Cold War and the Information Age, on the way in which disinformation was perceived as a problem and which counter measures were taken by the US. The literature analyzed in this literature review in combination with the aim of this thesis led to the following research question: "*What factors shaped the United States' attitude towards Russian disinformation during Operation InfeKtion (1980s) and the Russian influence campaign in the United States in 2016 and how can the differences and similarities between these time periods be explained?"*

2.2 Conceptual Framework

2.2.1. Disinformation and Active Measures

In this thesis, disinformation will be defined as "The dissemination of deliberately false information, esp. when supplied by a government or its agent to a foreign power or to the media, with the intention of influencing the policies or opinions of those who receive it." (Cheyfitz 2017, 15) This definition was chosen because it highlights the intention to cause harm as well as highlight government involvement. Disinformation is part of 'active measures' which in this thesis will be understood as explained by Thomas Rid. First, active measures are methodically planned by large bureaucracies and not just unplanned lies made up by politicians. Second, an element of disinformation is present in all active measures. Third, active measures always have a goal which usually revolves around weakening the target (Rid 2020, 16). In short, active measures are tools that require a methodical planning before use and are used by state and non-state actors which are aimed at weakening the target. Disinformation is one of these tools.

2.2.2. Cold War

The term Cold War refers to a time period after the Second World War in which the international order entered a new bipolar system which was characterized by a power struggle between the US and the Soviet Union (McMahon, 2009, 1) This power struggle with the Soviet Union became the main motivator behind American foreign affairs and is now known as the Cold War (Jeansonne & Luhrssen, 2014, 82).

2.2.3. Information Age

The information age refers to the current age. This time period is characterized by the use of (information) technology which is rapidly developing and increasingly influencing daily lives (Soma, Termeer, and Opdam 2016, 89). The information age also symbolizes "a shift from production-oriented to service-based occupations, the manipulation of symbols, and a decrease in the percentage of the labour force involved in the production of tangible products. Most importantly, society is characterized by the emergence of 'networked individualism' in which the likelihood of connectivity beyond the local group increases drastically." (Mesch and Talmud 2010, 2)

2.2.4. National Security

A concept which may not have been explicitly mentioned up to this point, but which lies at the foundation of the disinformation problem, is national security. Throughout this thesis, national security is understood as 'the preservation of territorial integrity and sovereignty of a state, as well as its core political and cultural values, against military threats from without and disruptive elements from within.' (Chandra & Bhonsle, 2015, 337)

3. Methods

This chapter will address the method of analysis used in order to answer the research question. An explanation of Securitization theory will be given as well as a brief overview of the questions that led to the chosen pillars of this research, problem perception and counter measures. The next section will be centered around introducing and justifying the case studies, Operation InfeKtion and the 2016 US presidential election, followed by the primary data at the basis of the analysis. This chapter will end by addressing possible limitations and strengths of this research.

3.1. Method of Analysis

The theoretical framework guiding the analysis is that of securitization theory. Balzacq defines securitization as "an articulated assemblage of practices whereby heuristic artefacts (metaphors, policy tools, image repertoires, analogies, stereotypes, emotions, etc.) are contextually mobilised by a securitizing actor, who works to prompt an audience to build a coherent network of implications (feelings, sensations, thoughts, and intuitions) about the critical vulnerability of a referent object, that concurs with the securitizing actor's reasons for choices and actions, by investing the referent subject with such an aura of unprecedented threatening complexion that a customised policy must be immediately undertaken to block it." (Balzacq, Léonard, and Ruzicka 2016, 495) In short, an issue is given a certain level of importance for the audience to believe it is an existential threat, this enables those in power to act on this issue in every way they see fit.

The origins of securitization theory can be found in International Relations. The founding father of securitization theory is Ole Wæver (Taureck 2006, 53), a professor in International Relations. Wæver noticed that around the mid 1980s there was a renewed interest in reconceptualizing security (Wæver 1995, 1). Wæver calls for a reconceptualization of the concept of security, since he does not agree with the traditional approach to security. Wæver, associated with the Copenhagen School of securitization, regards securitization as a speech act. "*In naming a certain development a security problem, the "state" can claim a special right*, one that will, in the final instance, always be defined by the state and its elites." (Wæver 1995, 6) Through this lens, securitization is a tool with which power and control can be gained over certain issues. The core concepts of securitization theory which this thesis will use are the 'securitizing actor', the 'referent subject' and the 'referent object'. The

securitizing actor is “the agent who presents an issue as a threat through a securitizing move” (Balzacq, Léonard, and Ruzicka 2016, 495), the referent subject can be defined as the presence that is threatening, and the referent object is that what is being threatened. Securitization theory also puts a lot of emphasis on context. Nowadays, scholars are not likely to ignore the influence of context in securitization theory because it “highlights how differences in the way securitizing moves are presented and/or received depend on the wider social environment.” (Balzacq, Léonard, and Ruzicka 2016, 504)

This thesis will use securitization theory to specify “how, and under which conditions, the security-ness of an issue is fixed.” (Balzacq, Léonard, and Ruzicka 2016, 517) In this case the issue at hand is disinformation. Based on the core concepts of securitization theory, this thesis will analyze the documents using the following questions. What was at stake? What was the threat specifically? Who made it into a threat? In what way was the threat viewed by the different groups involved? What did those in charge have to focus on in relation to countering the threat? Who were involved in the process of problem perception and counter measures? Does anyone benefit from the threat? These questions will be applied to the case studies and documents later specified. In order to (partially) answer these questions, this thesis will occasionally make use of discourse analysis. In simple terms, discourse analysis is the analysis of language, spoken and written. “Discourse analysis reads beyond the text per se and tries to understand the underlying conditions behind the problem by extending the perspective of inquiry.” (Tari 2011, 461) Discourse analysis allows the reader to read between the lines and link texts to other issues at hand. Discourse analysis will be applied to the case studies and documents in order to create a scope that will help answer the previously posed securitization theory questions. For example, discourse analysis allows for a better understanding of why certain counter measures were, or were not, taken in a time period. It considers other factors at play in for example the Cold War, that could explain why the US, at first, had a mainly defensive attitude towards foreign influence activities. In the final chapter, this thesis will use the method of comparison to compare the findings of the previous chapters on problem perception and counter measures in the Cold War and in the Information Age to see if any factors can be identified that shaped the US’ attitude towards Russian disinformation and how these factors might be similar or different depending on the time period.

These questions that are derived from securitization theory also form the basis of the two main areas of focus in this thesis, problem perception and counter measures. This research decided to put part of the focus on problem perception because to fully understand

the extent of a threat, one needs to have knowledge of how the problem is perceived by those involved. The questions posed by securitization literature provide information that will most likely lead to the understanding of how the problem is perceived. These same questions also provide information as to what counter measures were taken to deal with the problem. The remaining focus is put on counter measures since they are an important aspect to understand since they reflect the US' attitude towards the problem.

3.2. Case Study Justification

This research will look at disinformation campaigns by Russia against the US. It will use these two countries for its analysis due to the fact that they were the two main actors in the Cold War. The Cold War was characterized by a power struggle between the US and the Soviet Union. In recent years, it has been argued that the world is heading for a new Cold War characterized by another power struggle between the US and Russia. The tensions between the US and Russia have been on the rise. Just like in Cold War times, Russia has been taking expansionary action against neighboring countries. In 2014, the Russian military entered Ukraine for what they called 'an intervention', which resulted in a lot of international debate on the possibility of a new Cold War (Gromyko 2015, 141). The similarities between the time periods surrounding these two nation states allow for a comparison which could potentially reveal information that could prove relevant in understanding the current tensions. Another reason for looking at Russia with regards to disinformation is simply because they are most often associated with disinformation.

Operation InfeKtion was a Soviet campaign set up in 1985 as part of the Soviet Union's active measures during the Cold War (United States Department of State 1987, 33). Operation InfeKtion came to light in 1987 when this disinformation campaign reached the American public through American media outlets (Ellick and Westbrook, n.d.). This disinformation campaign was aimed at convincing the world that the American government had secretly designed the AIDS virus in their lab at Fort Detrick in order to use it as a biological weapon against gay and black people (Boghardt 2009, 4-5; Ellick and Westbrook, n.d.). The Soviets had planted this piece of disinformation in an Indian newspaper and after some time published it in their own newspapers (Boghardt 2009, 4-5), citing the Indian paper as their source. Over the course of several years this story was passed around the African continent before it reached the US in 1987. The same year, the AMWG published their report on Soviet Active Measures, including a detailed chapter on exposing Operation InfeKtion (United States Department of State 1987). There are several reasons for choosing Operation

InfeKtion as a case study. The first one being that Operation InfeKtion has been well documented over the years (Rid 2020, 15). Second, through Operation InfeKtion the American public came into contact with large scale disinformation campaigns for the first time. Big disinformation cases like this led to the creation of the AMWG which consequentially published a report on Operation InfeKtion.

The second case selected is the Russian disinformation campaign surrounding the 2016 US presidential elections. Russian disinformation is said to have played a role in the outcome of the US elections (Nemr and Gangware 2019, 18). Influencing US politics has been a Russian objective since the Cold War (Bittman 1985, 47). In 2016, Russia launched an elaborate campaign to discredit Clinton and support the candidate they deemed more favorable to Russian objectives, Donald Trump (Walton 2019, 107). This campaign launched by Russia included criminal acts such as hacking government officials to leak and manipulate private information (Ellick and Westbrook, n.d.) but also disinformation practices on the internet through bots and trolls (Nemr and Gangware 2019, 14). Some have called this campaign Operation Secondary InfeKtion (The DFRLab Team 2019). The reasons for selecting this case study are as follows. First, this case has been well documented. Since news broke of possible Russian meddling in the elections many have researched and written about it. Which leads to the second reason, the official investigation. The US government launched an official investigation into the matter which produced a five-part report, of which parts will be used in this research.

3.3. Data Justification

To answer the research question, this thesis will make use of primary data as well as additional secondary data. Intending to gain a better insight into the time period surrounding Operation InfeKtion the following sources will be used:

- Soviet Influence Activities: A Report on Active Measures and Propaganda, 1986-87' This document, published in 1987, was created by the AMWG as an update to a previous report submitted to congress on Russian active measure campaigns. This document discusses the Soviet active measures apparatus as well as ways in which the Soviet Union has conducted active measures in the US. In this document, special attention is paid to Operation InfeKtion.
- 'Soviet Active Measures in the United States – an Updated Report by the FBI' This document is an Extension of Remarks from the Congressional Record. This document

contains the speech by Hon. C.W. Bill Young of Florida in the House of Representatives. In this speech Mr. Young advocates for more public awareness of Russian active measures of which disinformation is a part. This document also contains the text of an FBI document on Soviet active measures in the US in 1986-87.

As for the Russian influence campaign of 2016, the following sources will be used:

- 'Report of the Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election. Volume 2: Russia's Use of Social Media with Additional Views' This document provides an insight into contemporary Russian disinformation practices as well as the US' government's response. This document has a specific focus on the use of social media surrounding the 2016 elections.
- 'Report of the Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election. Volume 3: U.S. Government Response to Russian Activities' This document follows the previously discussed document and describes the actions taken and considered by the US government against Russian active measures in 2016.

The first two documents have been selected due to the fact that they deal with Soviet active measures in the US in the Cold War and because they are official government documents. The same criteria led to the selection of the other two sources. The only difference being that the Cold War was replaced by the information age. Due to the fact that these four documents are official government documents it will help the discourse analysis since they are all written from the same perspective of the US government.

All sources, both primary and secondary, have been selected because they hold information that helps work towards an answer to the research question. The bases of the analysis rest upon the primary sources, the secondary sources will be used to support the findings of the primary sources. What this research hopes to achieve by analyzing these sources is identifying differences and similarities with regard to problem perception and counter measures between the cases. This could valuable in understanding disinformation practices and could help prevent "repeating mid-century errors that are already weakening liberal democracy in the digital age." (Rid 2020, 16)

3.4. Strengths and Limitations

The strengths of this research lie in the fact that unlike most previous disinformation research this research combines different fields of study. This way the sources are analyzed from different perspectives which may lead to interesting findings and conclusions. This research also has a comparative aspect which allows similarities and differences between the two cases in the two time periods to be identified and analyzed.

Almost every type of analysis is accompanied by some limitations. In the case of discourse analysis this means that the findings are based on the authors interpretation of the analyzed texts. Therefore, if this research were to be replicated findings might slightly differ. Author's bias is not the only potential bias that could influence this analysis. As previously stated, this thesis will make use of government documents of the US. Government documents are always biased. The US' interpretation of Russian disinformation will differ when compared to, for example, the Russian interpretation. The same applies to the method of comparison. Another limitation of this research is that the primary sources on the Russian influence campaign of 2016 are partially redacted due to the case being so recent.

4. The American Attitude and Problem Perception

In this chapter, the documents will be analyzed in order to determine how the concept of problem perception is visible through them. The documents will be analyzed through several questions. What was at stake? What was the threat specifically? Who made it into a threat? In what way was the threat viewed by the different groups involved? What did those in charge have to focus on in relation to countering the threat? Who were involved in the process of problem perception and counter measures? Does anyone benefit from the threat? The answers to these questions will reveal how the US looked at active measures and in particular disinformation. More precisely, what factors shaped their attitude towards these problems. Section 4.1 centers around the late Cold War with a special focus on the disinformation campaign known as Operation InfeKtion. Section 4.2 is about the information age with specific focus on the 2016 presidential elections in the US.

4.1. Problem perception in the late Cold War

4.1.1. How are active measures perceived as a problem?

The document written by the AMWG defines active measures as "a literal translation from Russian, *aktivnyye meropriyatiya*, which denotes covert or deceptive operations conducted in support of Soviet foreign policy." (United States Department of State 1987, viii) In the Congressional Records Extensions of Remarks, active measures are defined as " a literal translation of a Russian phrase used to describe overt and covert techniques and intelligence operations designed to advance Soviet foreign policy objectives and to influence events in foreign countries." (Young and Federal Bureau of Investigation 1987, 4717) When comparing these two definitions it is interesting to note that both mention that the term active measures comes from a literal translation of the Russian language. This illustrates that both documents associate the practice of active measures with the Russians. Another interesting aspect is that they both mention that active measures are used to support Soviet foreign policy. They specifically state that active measures are used in support of Soviet foreign policy which one could interpret as them believing that active measures are a weapon primarily used by the Soviet Union to advance their interests.

The US view the Soviet Union to be the main benefactor of active measure campaigns. Through several different ways, the Soviet Union tries to isolate the US in the international climate while creating an appealing and improved Soviet image (United States Department of State 1987, 84; Young and Federal Bureau of Investigation 1987, 4717). These active

measures were specifically used to “disrupt and undercut U.S. policies, sow suspicion about U.S. intentions, and undermine U.S. international relations.” (United States Department of State 1987, 29) This meant that Soviet active measures had the potential of diminishing trust in the US’ political, economic and military programs both on a national and international level (Young and Federal Bureau of Investigation 1987, 4717). This decreasing level of trust in the US is something the government wants to prevent. Securitizing the Soviet Union and their active measures allows the government to deploy extraordinary measures to counter these threats. This illustrates that the US, in their role as the securitizing actor, has the power to shape the attitude of the whole nation towards active measures and disinformation through their power to make something into a threat to national security. Using the term national security in the US creates a sense of fear among the public which gives the government the power to use extraordinary measures against the threat.

Another similarity between the documents is that they both highlight the ways in which the Soviet Union tries to achieve the disruption of the US’ image. These ways all rely on the principle of exploiting already existing tensions (Walton 2019, 110; Bittman 1985, 47), giving a psychological dimension to active measures. The US is a nation with many different groups which sometimes causes friction. These tensions between groups can be easily influenced by active measures. Bittman specifically highlights this stating that US internal affairs should be disturbed by the use of active measures through for example conducting “operations that create racial tensions within American society” (Bittman 1985, 47). Through this method, the Soviet Union found a way to internalize the threat. Active measures campaigns are no longer aimed at the entire US population but sometimes just at specific racial or religious groups. When the active measures campaign is aimed at a smaller group it becomes harder for the people to label active measures as a national security problem. The US population is feeling increasingly separated from their government through a loss of trust and are putting their individual security above national security. This lack of trust could lead to a very instable nation state, which is what the Soviet Union was aiming for. The feelings of insecurity that arose within, for example, racial subgroups in the US, give rise to a different perspective on active measures. A perspective of an internal threat instead of external. This leads to the argument that these subgroups have an impact on the attitude of the US towards active measures and disinformation.

To conclude, the view in both documents is that the Soviet Union is the main threat, also known as the referent subject, to the US. The referent object presented throughout both these documents is the threat to the position the US held in the international order. Although

not specifically mentioned, one can interpret this as a threat to the national security in the US. By applying the securitization process to Russian active measures campaigns the US gained the power to use extraordinary measures in their pursuit to counter them. The US government can in this case be seen as the securitizing actor as well as a benefactor. As for factors that shaped the attitude of the US towards active measures, one could state that the US government, as the securitizing actor, is a driving force behind shaping the US' attitude. One could also make an argument for the influence of subgroups within society on the public attitude towards active measures.

4.1.2. How is disinformation perceived as a problem?

In the documents the focus is on active measures in general. Both documents view disinformation as a part of active measures. Therefore, many of the answers to the guiding questions in this section will be the same as the section on active measures. The document written by the AMWG defines disinformation as "a deliberate attempt to deceive public or governmental opinion, can be oral and/or written." (United States Department of State 1987, viii) In the Congressional records Extensions of Remarks, disinformation is not explicitly defined, however, it is mentioned as one of the principal forms of active measures, illustrating the importance of the issue (Young and Federal Bureau of Investigation 1987, 4717).

The documents link disinformation to the practice of making forgeries. Due to the illegal aspects surrounding forgeries, the word has a negative connotation. Linking disinformation to forgeries is therefore a good securitizing tactic since the negative connotation of forgeries (partially) transfers to disinformation. As the AMWG report states, "forgeries are an effective means of spreading disinformation." (United States Department of State 1987, 29) According to the Congressional Records Extensions of Remarks, "forgeries are often designed to supply the 'factual evidence' needed to prove the disinformation that Moscow has already advanced through other active measures operations and propaganda." (Young and Federal Bureau of Investigation 1987, 4717) This statement shows the vastness of the disinformation machine in which disinformation is created to support other disinformation pieces. Part of the power of forgeries lies in the fact that they repeat the 'original' disinformation. Disinformation can easily cause a lot of damage just by being repeated and shared (Nemr and Gangware 2019, 2), even when it is repeated by people who are debunking it. Repetition of a story makes it more real to many people (Ellick and Westbrook, n.d.). For example, even though the story that aids was created by the US government in a lab has been

widely debunked, many people in the US still believe it is true since it is referred to in contemporary music and on TV (Ellick and Westbrook, n.d.).

The origin of forgeries as a form of disinformation is hard to determine. However, most forgeries do seem to support Soviet interests (United States Department of State 1987, 29). Most forgeries share an underlying theme: "The U.S. will carry out foreign political military, and economic activities in complete disregard of foreign public opinion and often at the expense of its allies around the world." (United States Department of State 1987, 29) In short, their purpose is to destroy the integrity of the US. Because of defectors like Ladislav Bittman, we now know that destroying the integrity of the US was one of the long-term goals of the Soviet disinformation campaigns. Bittman describes this goal as, "The United States remains the 'main enemy' and major target. As such, it must be continuously discredited as an imperialist, neocolonialist power threatening world peace and the economic well-being of other nations." (Bittman 1985, 46) Disinformation is a powerful tool used to discredit others and swing public opinion. Attacking US integrity would not only result in a weakened enemy on the domestic front, but it would also help lower the enemy's prestige in the international community. The actor behind the disinformation and the potential damage both attribute to the way in which the threat perceived. It is this perception of the threat that shapes the way in which the US reacts to disinformation. A higher potential damage leads to heightened threat perception which in turn most likely results in a more intense reaction to the threat.

Applying the guiding questions to these documents reveals that both believe the Soviet Union to be the referent subject. The referent object, as well as the securitizing actor, also corresponds with those identified in the active measures section. The insights surrounding disinformation show that both documents regard disinformation as a piece of the active measures threat, therefore the documents are more specified in what the threat specifically is through examples such as forgeries. Although the origin of forgeries is hard to determine, they, in most cases, seem to support a view that is favorable of the Soviet Union. This makes the Soviet Union look like the main benefactor. As for the factors that shaped the US' attitude towards disinformation one could argue that the way a threat is defined and perceived is of importance.

4.1.3. Operation InfeKtion

Operation InfeKtion was a Soviet campaign set up in 1985 as part of an active measures campaigns during the Cold War (United States Department of State 1987, 33). This

disinformation campaign was aimed at convincing the world that the American government had designed the AIDS virus at Fort Detrick in order to use it as a biological weapon against black and gay people (Boghardt 2009, 4-5; Ellick and Westbrook, n.d.). This piece of disinformation was first published in an Indian newspaper, later finding its way to the African continent as well as the Soviet Union, all stating the Indian newspaper as their source (Boghardt 2009, 4-5). In the year 1987, this disinformation campaign reached the US.

Operation InfeKtion is one of the most well-known cases of disinformation from the late Cold War. This could be attributed to the fact that it was widely debunked at the time, making it well-known and also because people are still referencing it today in music from artists like Kanye West and on TV shows (Ellick and Westbrook, n.d.). One of the groups concerned with debunking this story was the AMWG. In their report they dedicate an entire chapter to this disinformation campaign. The document from the Congressional Records does not pay as much attention to this specific case; however, they do seem to support many of the claims made in the AMWG report on for example the dangers of large disinformation cases.

As previously stated, the origin of this disinformation campaign can be traced back to an Indian newspaper, the Patriot (United States Department of State 1987, 34). However, the Soviet Union is seen as the main perpetrator behind this campaign. The Indian newspaper is one of many that have been previously linked to spreading news in favor of the Soviet Union in exchange for payment (United States Department of State 1987, 38). In order to hide their involvement, the Soviet Union wrote an anonymous letter to the Indian newspaper, pretending to be a scientist working at Fort Detrick. The Indian newspaper then published the information in the letter and was later cited by larger Soviet news agencies who reported on the story.

To give this campaign more credit, the Soviet Union exploited the lack of access the developing world had to the Western news agencies (United States Department of State 1987, 38). These nations, most of them located in Africa, Asia and Latin America, could not afford contracts with Western news agencies, they, however, could afford contract with news agencies of Soviet origin (United States Department of State 1987, 38). This meant that after the Soviet Union took the story from the Indian newspaper, they were able to spread it to many more countries in the developing world. This relates back to the statement that disinformation can gain a certain amount of power just by being repeated and shared (Nemr and Gangware 2019, 2).

This power through repetition also brings along higher levels of danger to the referent object. In the case of Operation InfeKtion, the referent object can be identified as either the

internal security of the US or their position in the international community. As for the internal security of the US, Bittman described in his book, US internal affairs should be distorted by "operations that create racial tensions within American society" (Bittman 1985, 47). Operation InfeKtion is a prime example of this since part of the disinformation campaign was the news that the US had created this virus in order to use it as a biological weapon against black people and homosexuals (Boghardt 2009, 4-5; Ellick and Westbrook, n.d.). Since a large part of the US population is black, the news that your own government has created a biological weapon to fight you has a big chance of resulting in high tensions coming from a heightened feeling of insecurity.

The position of the US in the international community was also threatened since many other nations would not like to be associated with a nation that has actively been creating a virus to destroy certain groups in their own society as well as outside their borders. Last was the idea that this disinformation campaign could hurt American military operations overseas and force them to withdraw from certain places, since part of the disinformation was that the spread of the virus could be linked to the places where the American military was stationed (United States Department of State 1987, 33).

In the previous section on disinformation, both documents stated that disinformation campaigns are often linked to forgeries, this too is the case for Operation InfeKtion. In this specific case, a forged press release supposedly from the German health minister stated that the US army hospital could not admit anymore civilian AIDS patients since it barely had enough room for their own men. This statement gives a certain level of credit to the claim that the US military is a source for the AIDS virus, which could lead to foreign countries being opposed to their presence within their borders, leaving the US military with a decreasing level of military influence overseas.

Another way the Soviets wanted to give credit to their claims was through scientific channels. In their news report, Soviet news agencies often quoted the work of an East-German, retired professor in biophysics, Jason Segal (United States Department of State 1987, 33). In his report, the retired professor "attempts to demonstrate through 'circumstantial evidence' that the AIDS virus was artificially synthesized at Fort Detrick in 1977 from two existing, naturally occurring viruses, VISNA and HTLV-1." (United States Department of State 1987, 33) Having a scientific report, even when based on assumptions and circumstantial evidence (United States Department of State 1987, 33), will help strengthen the notion of legitimacy surrounding the disinformation. The report tries to decrease the credibility of this professor by emphasizing that his argument is based on 'circumstantial

evidence'. Terms like 'circumstantial evidence' are used to create a feeling of doubt surrounding the claims made by the professor.

The referent subject in this case is the Soviet Union as well. Even though they tried to hide their involvement by spreading the disinformation through foreign news media outlets, the disinformation campaign can still be traced back to the Soviet Union. Spreading the campaign through a large number of foreign news media outlets also had the benefit of creating a sense of legitimacy through repetition. A sense of legitimacy was also aimed for by involving the work of retired scientist professor Jason Segal, even though his work that stated AIDS was a man-made virus was based on assumptions and circumstantial evidence. The referent objects in this case are identified as the internal security of the US and their position in the international community. Through stating that the virus was specifically designed to hurt black people and homosexuals, the Soviet Union created the perfect platform for internal tensions. By spreading forgeries that insinuated that the US military was a source for spreading the virus the Soviet Union managed to create the notion that it was better not to have any US military presence within your borders if you wanted to stay save from the virus. This notion benefitted the Soviet Union because it in theory would lead to a lower standing of the US in the international order. One could argue that Operation InfeKtion was in itself a factor that shaped the US' attitude towards disinformation because this case was the first major case of disinformation to become well-known amongst the American public.

4.1.4. Discussion

The attitude shaping factors identified in this section are the securitizing actor, subgroups within society, the level of threat perception and major cases of disinformation such as Operation InfeKtion. The influence of the securitizing actor on the attitude towards a security issue like disinformation is not unheard of and can be easily explained by securitization theory. The securitizing actor determines which issues become security threats and which threat level is assigned. This gives the securitizing actor great influence over the attitude towards a security threat. The level of threat perception can be seen as a sub-factor of the securitizing actor. The level of threat perception largely determines the attitude of a nation towards the disinformation threat; however, the securitizing actor is heavily involved in influencing that level of threat perception. Even though the securitizing actor and threat perception may be obvious factors in shaping the attitude of the US, they do illustrate the need to understand the securitization process of an issue, if one wants to understand how and

why certain reactions, or the lack thereof, took place. This could prove important in comparable, future situations.

Literature on disinformation often speaks of the targeting of marginalized groups within a society. This combined with the fact that in securitization theory emphasis is put on context because it "highlights how differences in the way securitizing moves are presented and/or received depend on the wider social environment" (Balzacq, Léonard, and Ruzicka 2016, 504) makes subgroups a more obvious shaping factor. Interesting to note is that even though subgroups are a noteworthy shaping factor, relatively little amount of literature deals with the influence of subgroups in combination with securitization theory and/or disinformation literature. This illustrates the need for more research that combines fields of literature related to the disinformation threat.

The last factor identified in the previous sections was the case of Operation InfeKtion. This factor too seems rather obvious because in most situations, people look back to history in order to find a similar event and base their attitude on what they learn from that situation. However, in the current literature, Operation InfeKtion mostly seems to be studied within a Cold War frame, which leaves its relevance to current disinformation cases often overlooked. Identifying a case like Operation InfeKtion as a shaping factor illustrates the need for more history-oriented approaches towards the disinformation threat, instead of the policy-oriented ones used by the US today.

The broader referent object identified throughout the documents is the threat to national security. More specifically, the documents mention the threat to the position of the US in the international order, the destruction of their integrity, disruption of their policies, and their internal security. The US has always been placed high on the international ladder. They like to see themselves as the leaders of the free world and have referred to themselves as 'the city upon the hill', meaning that they are the example that other nations look up to. They see themselves as unique and different, a superior nation that others should aim to be like. This is known as 'American Exceptionalism' (Ramrattan and Szenberg 2017, 222). American exceptionalism greatly influences the level of threat perception illustrated by the fact that it has often been a driving factor for the US to go to war. This in turn greatly influences the referent objects. As soon as an actor does not fit with the notion of American exceptionalism, through for example threatening US integrity or their international position, they can easily become a referent object.

The documents analyzed are mostly focused on Russia as being the main actor behind the disinformation threat. They explicitly state that disinformation is something which

benefits Russian interests and is designed to advance Russian foreign policy (United States Department of State 1987). They also explicitly link disinformation and active measures to Russia by stating that these terms originated in the Russian language. In the Cold War, stating an issue to be of Russian origin was a highly effective securitization tool since US- Russian relations were already tense. This way the referent object could be used by the securitizing actor to gain more power, since in securitizing an issue, the securitizing actor gains power and control over an issue and is allowed to use extraordinary measures.

4.2. Problem Perception in the Information Age

4.2.1. How are active measures perceived as a problem?

The Soviet Union may have disintegrated in 1991, but Russia did not stop their active measures practices (Ellick and Westbrook, n.d.) In volume two of the report on the Russian active measures campaign of 2016, more commonly known as the Mueller report, the authors acknowledge the fact that Russia is still carrying out active measures today (Selected Committee on Intelligence United States Senate 2019a, 12). In the document it is not clearly defined what they refer to when speaking about active measures, however, when reading the document one can get a sense of what the authors associate with the term active measures. First, they ascribe the practice of active measures to Russia by quoting a retired KGB general who said that active measures are "the heart and soul of Soviet intelligence" (Selected Committe on Intelligence United States Senate 2019a, 12). Second, the authors state that the aim of the active measures is to weaken the US' position in the international order. This in order to secure a more favorable position for Russia in the international community when a war between the two countries does happen. Third, the authors mention the exploitation of already existing tension in order to reach their goal, which, as previously discussed, can cause a threat to become an internal one as well as external. One could argue that internal struggles or the level of unity felt within a country as a result of these internal struggles is of great importance when battling a threat such as active measures. Having to fight an outside threat like active measures is a large undertaking, having to deal with internal struggles at the same time greatly influences the level of attention paid to the outside threat.

Active measures have long been a part of the Russian toolkit, however, there now seems to be a shift towards developing tools as part of 'information warfare' (Selected Committee on Intelligence United States Senate 2019a, 13). Information warfare refers to the deliberate manipulation of the information sphere in order to reach the same objectives as

with active measures. Using a term like ‘warfare’ to describe a threat gives it adds to the credibility of the threat, since the term is associated with past events with a high threat level. Information warfare has been a very effective tool for the Russians to reach their goal since it is extremely hard to defend against and because it is possible to produce large-scale operations at a lower cost.

These cheaper, large-scale operations have been largely due to technological advancements. One of these technological advancements was the internet. The internet has become such an important factor in active measures operations that Russia has established an organization called The Internet Research Agency (IRA), which carries out active measures campaigns at the orders of the Kremlin (Selected Committee on Intelligence United States Senate 2019a, 22). These active measures carried out by the IRA were not only physical but also virtual in nature. This brought along a new kind of threat, the cyber threat. Cyber-attacks allow for important information to be obtained by criminals and other opponents. As Bittman said, every good actives measures or disinformation campaign contains a bit of the truth (Ellick and Westbrook, n.d.). Using information obtained through a hack and spinning it to fit your narrative makes for a more believable active measures campaign which in turn will be more likely to succeed. Using words like ‘hacking’ also gives more credibility to the threat, since it is a largely illegal practice and therefore largely perceived as bad or threatening.

Russian active measures in the information age still form a threat to the international position of the US, however, with the emergence of, and the increased access to, the internet, active measures have become increasingly dangerous to the domestic affairs of the US. The internet allows for easier access to certain groups within a population, for example, smaller racial groups within the US. As previously stated, “operations that create racial tensions within American society” (Bittman 1985, 47) are one of the main objectives of active measures. This objective stems from the Cold War, however, it is still being pursued today (Walton 2019, 112). Active measures campaigns aimed at specific groups can cause the US population to feel increasingly separated from their government and lead them to put their individual security above the national security. A divided enemy nation is beneficial to the aggressor since such a nation is less likely to be able to defend their interests properly or interfere with anything they deem ‘wrong’ in the international community. Therefore, one could argue that the level of unity experienced within a nation influences the attitude a nation has towards a threat, in this case active measures.

When finished analyzing the documents in regard to the research question the following conclusions can be drawn. Even though some believed that the threat of Russian

active measures had disappeared with the disintegration of the Soviet Union, Russia never stopped their active measures and is still the main actor in these campaigns. The term active measures is still being used, however, one could argue that the term is slowly being replaced. For example, by terms such as information warfare, which hold more meaning to the public and are therefore more likely to raise the level of threat perception. Technological advancements have led to new ways in which to conduct active measures, such as through the internet. The use of the internet has given rise to a new perception of the threat. The main threat surrounding active measures is beginning to shift from national security to individual security due to the fact that the internet allows for the targeting of more specific audiences. Reaching specific audiences with these campaigns can lead to an increased feeling of separation between the government and the population and a division within the population itself. One could argue that a feeling of unity within a nation is instrumental in shaping their attitude towards problem. In the case of active measures, the problem might not get the attention it needs when there are high-rising tensions between groups within the nation's borders.

4.2.2. How is disinformation perceived as a problem?

The rise of technology has been commonly associated with disruption (Nemr and Gangware 2019, 2). While technology is meant to help industries advance it has often resulted in major disruption of industries. Not only has technology had its disruptive influence on regular industries like retail and media, but it has also left its mark on the disinformation industry (Nemr and Gangware 2019, 2). Social media has transformed the way in which disinformation can be spread, but also altered the credibility of the disinformation. The internet provided a way in which information was more easily accessible for everyone, everywhere, anytime. The internet also provided a place for people to more freely express their opinions and find other likeminded people (Schiffrin 2016, 117). In the early years of social media platforms people believed that they would 'bring democracy to the world.' (Schiffrin 2016, 117) They allowed for people in oppressed situations to come together and unite for their cause which has led to many protests in the name of democracy. However, this has also worked the other way. People with less than honorable intentions have found each other on the internet and conspired to commit violent acts as well as convincing others to join their cause. The internet has become a tool which is able to create a feeling of unity as well as take this feeling away. The internet could proof to be of influence in shaping the attitude of

nation towards a threat since its ability to influence the feeling of unity in turn influences the level of threat perception.

Although the authors of the analyzed documents do not provide a specific definition of disinformation, they do highlight several characteristics of disinformation in the information age. The first one highlighted is the fact that disinformation is spread at high volume and on multiple channels (Selected Committee on Intelligence United States Senate 2019a, 16). One of the main platforms used for the spread of disinformation in the Information Age is the internet, more specifically, social media. Social media platforms are easily available to many and are, with a few exceptions, not limited to geographical borders. This means that disinformation campaigns have the potential of reaching further with less effort (Nemr and Gangware 2019, 2). Social media also allows for a high volume of accounts that can spread the disinformation. This high volume is meant to overwhelm the target audience to such an extent that they can no longer distinguish between what is real and what is disinformation (Selected Committee on Intelligence United States Senate 2019a, 16). The multiple channels aspect of disinformation allows for easier repetition of the disinformation campaign. As previously stated, disinformation can easily cause a lot of damage just by being repeated and shared (Nemr and Gangware 2019, 2). The second characteristic identified in the report is the merging of overt and covert operations (Selected Committee on Intelligence United States Senate 2019a, 16). An example of this is the use of social media accounts to spread documents previously obtained through a hack. The third aspect is that of speed (Selected Committee on Intelligence United States Senate 2019a, 17). Speed is of high importance to the success of the disinformation campaigns. The speed with which disinformation is disseminated and shared is far higher than the speed with which governing bodies can react to the threat. Fourth is the use of automated accounts and bots (Selected Committee on Intelligence United States Senate 2019a, 18). The use of automated accounts and bots in combination with the man-operated accounts allows for high speed dissemination of disinformation in higher volumes than when using only man-operated accounts. The fifth aspect is the use of internet ‘trolls’ in order to hide Russian involvement (Selected Committee on Intelligence United States Senate 2019a, 18). An internet troll can be defined as “a real person sitting behind a keyboard who posts inflammatory, aggressive, harassing, or misleading messages online in an attempt to provoke a response from other users of social media.” (Selected Committee on Intelligence United States Senate 2019a, 18) In several cases, such as the influence campaign on the 2016 Presidential elections, trolls have been paid in order to get involved (Nemr and Gangware 2019, 14). Sixth and last aspect is the

manipulation of real people and events (Selected Committee on Intelligence United States Senate 2019a, 20). To be more specific, hired trolls target specific individuals and urge them to get involved in a certain matter in order to, for example, increase tensions within a nation even more (Selected Committee on Intelligence United States Senate 2019a, 20). As previously mentioned, these increased tensions lead to a decreased feeling of unity within a nation. This hurts the nation in multiple ways. First, they are divided internally which can cause problems that lead to instability within the nation. Second, due to the internal struggles, there is less room for foreign policy and the nation might lose their status in the international order. Third, due to the increased attention paid to the domestic threat, the nation becomes more vulnerable to threats from the outside. Therefore, one could argue that the level of unity within the nation is key in shaping its attitude towards a threat such as foreign disinformation, since less attention is paid to such threats if the domestic situation is unstable.

These aspects of disinformation as highlighted in the documents can lead one to draw the following conclusions. Just as with active measures in general, the focus of disinformation seems to have shifted from the national to the individual level. Individuals are being targeted by trolls to either unknowingly participate in a campaign or they are being aggravated in order to increase tensions in the community. With the use of trolls, the disinformation sector has gotten a new benefactor. Trolls are often getting paid for services, thereby benefitting from the high number of disinformation campaigns. Just as in the previous one, this section illustrates that that a feeling of unity within a nation is instrumental in shaping the attitude of a nation towards problem. Tools such as the internet can be identified as valuable in the process of influencing the feeling of unity.

4.2.3. United States Presidential elections of 2016

In 2016, Russia launched an elaborate campaign to discredit Clinton and support Donald Trump (Walton 2019, 107). This campaign launched by Russia included criminal acts such as hacking government officials to leak and manipulate private information (Ellick and Westbrook, n.d.) but also disinformation practices on the internet through bots and trolls (Nemr and Gangware 2019, 14). Some have gone as far as calling this active measures campaign Operation Secondary InfeKtion (The DFRLab Team 2019) referring to similarity in scale to the 1980s operation as well as the similar objective to discredit the US. During this more recent campaign, Russian operatives associated with the IRA conducted disinformation operations mainly through social media (Selected Committee on Intelligence United States

Senate 2019a, 3). The fundamental goal of this disinformation campaign was to influence the outcome of the presidential elections. Having a foreign entity trying to influence your elections is a threat on its own. But the means used to reach this goal also bring along a set of security risks. Part of the definition of national security is the preservation of the sovereignty of a state (Chandra & Bhonsle, 2015, 337). What this means is that when Russia started their campaign to influence the elections the national security of the US was being threatened. One of the ways in which the election was to be influenced was through the exploitation of already existing tensions within the US. For example, previously mentioned trolls were used to "polarize Americans on the basis of societal, ideological, and racial differences" (Selected Committee on Intelligence United States Senate 2019a, 3). The polarization of the different subgroups within the US can cause them to turn against each other or turn against the state due to a lack of trust. A side effect of this instability resulting from polarization is a decrease of influence in the international community. One could state that a campaign like the influence campaign of 2016 does not only influence the presidential elections, but also influences domestic affairs, diminishes levels of trust in government and threatens one's position in the international community.

In the case of the 2016 Presidential elections, it took the US some time to fully understand the scope of this active measures campaign as well as its aim (Selected Committee on Intelligence United States Senate 2019b, 4). The Mueller report found that in 2016 there was relatively no concern for electoral interference and therefore there was little to no attention paid to the threat (Selected Committee on Intelligence United States Senate 2019b, 4). One could argue that the US was caught in what is known as the sheer-nerve scenario. The sheer-nerve scenario entails that one does not think a certain threat to really happen on the basis of thinking they would not have the sheer nerve to do whatever the threat is, this often leads to leaders making wrong estimates in regard to the enemies intentions (Baudet et al. 2017, 162). In this case, the US did not think Russia had the sheer nerve to interfere with the elections after being repeatedly warned not to and therefore their attitude towards the threat was not an active one. However, the US overestimated their power and underestimated the willingness of Russia to have a pro-Russian American president.

Research done by the Mueller investigative committee revealed that many of the accounts that were used to spread the disinformation were associated with the IRA, which is a known affiliate of the Kremlin (Selected Committee on Intelligence United States Senate 2019a, 5). Listed in the findings of their research, the committee states that not only is the IRA an affiliate of the Kremlin, in this case they were explicitly tasked and fully supported by

the Russian government in their efforts to influence the elections (Selected Committee on Intelligence United States Senate 2019a, 5). More interesting findings from the research committee were that the IRA's main focus was on dividing the US through race or related issues (Selected Committee on Intelligence United States Senate 2019a, 6). The results of the research showed that 66% of the posts made by the IRA contained the term race or a term associated with race. The research also found that African-Americans were the group most targeted by information operatives of the IRA (Selected Committee on Intelligence United States Senate 2019a, 6). Another interesting finding was that the IRA actively involved the American public in their campaigns. For example, people were targeted to sign petition and the Trump campaign was contacted for help with the organization of a rally in support of his campaign. Involving the public is a way in which a nation can be divided which can lead to a decreased feeling of unity, a factor previously identified to be of importance in shaping the attitude of the US against disinformation.

The influence campaign of 2016 was one of the most recent large-scale disinformation campaigns in the US that we know of. The clear referent subject in this case was Russia. The Russian government tasked the IRA to set up an elaborated disinformation campaign that would divide the American Public and influence the election results in favor of the candidate that was more convenient for the Russians. The referent object in this case was in the first place, national security. An important part of national security is the protection of sovereignty. Having the elections influenced by a foreign actor harms a nation's sovereignty. Another referent object was domestic stability which was being threatened through the use of polarizing tactics. The case of the 2016 Presidential elections illustrates once again that level of unity is important in shaping the attitude of the US towards disinformation. A newly identified factor is the attempt to estimate capabilities, willingness and intentions. In this case the US underestimated the intentions and willingness of Russia, the sheer nerve scenario, which led them to not see electoral interference campaigns as a relevant threat.

4.2.4. Discussion

The attitude shaping factors identified in this section are the level of unity within the nation, the level of understanding of the problem and the estimate made of the capabilities, willingness and intentions of the referent subject. The level of unity as a shaping factor has been previously explored in the literature. Disinformation has been said to threaten social cohesion and increase polarization within society (Hendricks and Vestergaard 2019, 69). The literature also refers to the Russian tactic to use disinformation to exploit already existing

tensions within society. This means that the level of unity determines the vulnerability of the US as well as their attitude towards the problem. A higher level of unity leads to less opportunities to exploit existing tensions, which in turn could result in a more relaxed attitude towards disinformation. It could also result in a stronger response to the disinformation practices that do still take place since the US needs less of their capacity to deal with internal problems.

Although not often mentioned, the level of understanding of the problem as a shaping factor has not entirely ignored by the literature. Often when referring to disinformation in combination with understanding the problem, the literature refers to how answers should be given to the questions of how to identify disinformation and how to counter it. However, some research focusses on 'immunizing' the population against disinformation by teaching to have a 'critical mindset' in schools (Andersson 2015, 4). Even though the literature calls for increasing the understanding of disinformation among the population, the US seems to largely ignore this call, especially when it comes to policy makers. One of the main ways in which to learn about something is to look at its history. Although the tools used to carry out disinformation practices have changed over time, the basis and the aim of disinformation have not changed. The US would be wise to invest more into educating both the public and policy makers on the history of disinformation. This way it becomes easier to identify disinformation and create more effective counter policies.

The literature often mentions the lack of insight into the opponent's intentions. However, their capabilities and willingness to use disinformation are less often discussed as being of importance in shaping a nation's attitude. In estimating the opponent's capabilities and willingness to attack, the US creates a certain set of expectations on what the opponent might do and adjust their attitude according to this set of expectations. The danger of this lies in the fact that the US could walk into the trap of the sheer nerve scenario. A scenario in which reality does not meet their expectations and they are caught off guard. Again, in this case an argument could be made for a more extensive study of historical disinformation cases, looking at the opponent's willingness to take certain actions as well as the capabilities they had at the time. Comparing past capabilities with present intelligence on capabilities could provide a more accurate estimate which, combined with the history-based estimates on intentions and willingness, could lead to an attitude towards disinformation which is less likely to fall victim to the sheer nerve scenario.

The broader referent object identified throughout the documents is the threat to national security. The same sub-threats of loss of integrity, domestic tensions and fall in the

international order can be identified. Where in the Cold War loss of integrity was discussed by analyzing the Russian attempt to sow suspicions about US intentions, in the information age it was discussed through the lens of meddling in the Presidential Elections. In the documents on the 2016 elections, the disinformation campaign is often referred to as an 'information warfare' campaign. Using the term warfare, triggers a response in people which automatically makes them feel more threatened. This is an effective securitizing move which will most likely result in more power for the securitizing actor.

In the Information Age, Russia is still seen as the main referent subject. Quoting high ranking Russian officials who state that disinformation is at the "heart and soul of soviet intelligence" in order to clearly ascribe the disinformation threat to Russia. Interesting to note is the focus on 'Russian-based actors'. In the information age most disinformation is spread by bots and trolls, whose affiliation is very hard to ascertain since they work for the highest bidder. It becomes harder to prove that a nation is behind the disinformation campaign. The document assigns the use of bots and trolls to Russia by referring to the so-called 'troll-farms' of the Russian IRA which is a known affiliate of the Kremlin.

4.3. Conclusion

This chapter started with a section on active measures and disinformation in the Cold War. In the part on active measures, the definition of the concept was discussed as well as other important aspects such as the main actor behind it and the implications for national security in the US. The next part on disinformation discussed how to define this concept as well as a specific form of disinformation, forgeries. The section on the Cold War ended with the analysis of the case of Operation InfeKtion, a Soviet disinformation campaign in which they tried to make the world believe that the US had created the AIDS virus. The next section discussed active measures and disinformation in the context of the information age. Both parts on active measures and disinformation detailed the influence of technological advancements on influence operations. Through these advancements, operations have become more fast-paced and larger in scale. In the last part of this section the case of the US 2016 Presidential Elections was discussed and analyzed. In this case, Russia tried to influence the US elections through disinformation, in order to secure the victory for the candidate they deemed more favorable to their interests as well as weaken the political stability in the US.

At the end of this chapter, the following conclusions can be drawn. In both time periods, as well as the specific cases, it was the Russian government that can be identified as

the main referent subject. The documents illustrate Russian involvement by referring to the Russian translation of important concepts, referring to the fact that disinformation seems to be designed to advance Russian foreign policy, quoting the statement that disinformation lies at the heart and soul of Soviet intelligence, and mentioning the fact that most non-government actors involved are known affiliates of the Kremlin. In most cases, the Russian government tries to hide involvement by either supplying someone with the disinformation to later quote them as a source, or by hiring someone else to execute their disinformation campaign. The referent objects identified can be summarized as national security, individual security and the international position of the US. The main goals of the Russians are to lower the influence of the US in the international community and create a more favorable attitude towards Russia, to exploit already existing tensions within the US to cause an unstable environment and to create a position in which the US is too weak and has not enough allies to win in case a war between the two nations does break out. Repetitive mentioning of these referent objects throughout the documents can be said to play into the population's feeling of 'American Exceptionalism'. This concept lies at the basis of American ideology, therefore, suggesting that someone is threatening this feeling has the potential to trigger an intense response in the population. Using terms like 'information warfare', the documents hope to trigger a feeling of fear which raises the population's level of threat perception with regards to disinformation.

The securitizing actor in most cases is the US government, however, in cases such as Operation InfeKtion and the influence campaign of 2016, it was one person or a small group from the intelligence community that first had to convince the rest of the government of the imminence of the threat. This does not mean that before the government did not perceive disinformation as a threat, however, they did underestimate it. Underestimating the threat is dangerous since a late reaction may have allowed for the disinformation to be spread further which makes it harder to fight.

As for the factors that shaped the US' attitude towards disinformation one could state that the level of threat perception, individual cases and securitizing actors such as the government are all instrumental in shaping the attitude towards disinformation. Other factors such as unity within the US, the level of understanding and policies derived from attempts to assess capabilities, intentions and willingness of the Russians are important as well. What these factors have shown is that research into the disinformation issue is growing, however, not enough. More research needs to be done, especially into historical cases of disinformation, in order to educate people on the issue and be able to properly defend against it.

5. The American Attitude and Counter Measures

This chapter will analyze the measures taken by the US to counter disinformation in the late Cold War as well as the information age. This will be done by looking for specific methods to counter disinformation in the documents. The counter measures found in this analysis will be used to determine which factors shaped the US' attitude toward disinformation. Section 5.1 is dedicated to the (late) Cold War. Section 5.2 contains the analysis of the information age.

5.1. Counter Measures in the Cold War

5.1.1. Government Policies on Disinformation

Most Cold War government policies were aimed at the 'Soviet threat'. The fear of the Soviet threat had risen to such high levels that a policy document was made which detailed what major threats the US and the free world were facing, and what could be done about it. This document is known as the NSC-68. In the NSC-68 policy document, the author highlights several possible courses of action to deal with the Soviet threat. The author suggests the possibilities of continuing the current policies, isolation and war as well as a rapid build-up of strength to prepare for the possibility of an attack (Department of State 1950, 44). The NSC-68 favors this last option because it "is the only course which is consistent with progress toward achieving our fundamental purpose." (Department of State 1950, 54) The idea of this option is to make sure that the US has the advantage in the political, economic and military sector to achieve what the document calls the 'frustration of the Kremlin design'(Department of State 1950, 54).

Around the 1970s a new idea was introduced into American Cold War politics. The idea, President Nixon wrote, was 'to involve Soviet interests in ways that would increase their stake in international stability and the status quo. There was no thought that such commercial, technical, and scientific relationships could by themselves prevent confrontations or wars, but at least they would have to be counted in a balance sheet of gains and losses whenever the Soviets were tempted to indulge in international adventurism." (Gaddis 2005, 308) This idea is now known as détente. Kissinger later stated that "Detente encourages an environment in which competitors can regulate and restrain their differences and ultimately move from competition to cooperation." (Gaddis 2005, 309) This new idea of détente was still one of defense instead of offense. This détente between the US and the Soviet Union was not a policy aimed at ending the competition for superiority between the two states, however, it was

put in place to make sure that this competition would not reach dangerous levels (Gaddis 2005, 310). The US wanted to prevent a nuclear war at all costs and in order to do that they believed they needed to follow defensive policies.

However, this all changed when Reagan was elected president. Reagan believed that the Cold War should be battled by using offensive measures. President Reagan was instrumental in the establishment of the AMWG, which was responsible for the investigation into Operation InfeKtion.

In order to actively counter disinformation, the US realized they should educate themselves more on this matter. Within the intelligence community, summits and hearings were held in order to educate intelligence operatives on the dangers of disinformation (Young and Federal Bureau of Investigation 1987, 4716). Most of the information on disinformation supplied to these intelligence professionals came from defectors, such as Ladislav Bittman. These defectors who had previously been part of the Soviet disinformation machine were able to provide valuable information into the nature and intentions of disinformation campaigns which helped the intelligence professionals better understand the problem (Young and Federal Bureau of Investigation 1987, 4716). A better understanding of disinformation is crucial if one wants to effectively counter it.

These informative meetings of intelligence professionals were often summarized and put in a report. A selection of these reports were published by the government in order to increase public awareness (Young and Federal Bureau of Investigation 1987, 4716). By increasing the awareness, the government aimed to improve the ability of the US to recognize Soviet disinformation campaigns and thereby actively diminish their effectiveness (Young and Federal Bureau of Investigation 1987, 4716). Increasing awareness was part of the RAP method. This stands for Report-Analyze-Publicize (Cull et al. 2017, 29). This method was the main counter measure taken by the AMWG was to discredit and debunk the disinformation campaigns. The RAP method dictates one should first report the suspected piece of disinformation, this is followed by thorough analysis done by intelligence professionals, and in the end the findings of the analysis are widely published in order to let the people know of this piece of disinformation. This method, however, was very time consuming due to the time it takes to properly analyze and refute disinformation, therefore it was not the most efficient way to counter disinformation.

To summarize, the early years of the Cold War where characterized by a defensive attitude towards disinformation. During the 1980's there was a shift from defensive towards offensive policies. This change was instigated by President Reagan. In those years, the Active

Measures Working was established to specially deal with the threat of Soviet active measures such as disinformation. At the same time, the intelligence community studied the threat in order to be better prepared to counter it. They learned from defectors that were previously involved in Soviet active measures operations as well as from colleagues who were tasked with monitoring and countering these operations. They also released documents to educate the American public and increase awareness which could lead to an improved ability to recognize the threat and reduce its effectiveness. As for the shaping factors, one could argue that the attitude is shaped by those who hold power such as the president. In this case of the Cold War, the attitude significantly changed when Reagan was elected president from a defensive to an offensive attitude.

5.1.2. Operation InfeKtion

When Operation InfeKtion reached the US, they began to work hard to contain the damage. In order to coordinate their efforts to counter these false allegations the responsibility was assigned to the Department of State, the department of Health and Human Services and the United States Information Agency (United States Department of State 1987, 41). In the beginning, when the story was first circulated in the Soviet media, the US Ambassador in Moscow immediately reached out to said media outlets with the information that the story they were publishing was false, however, the media outlets decided to ignore the ambassador (United States Department of State 1987, 41). The US had their ambassadors and other public affairs officers reach out to other media outlets around the world who had published this story (United States Department of State 1987, 41-42). Many of these media outlets then retracted the story and published a rectification. In addition to approaching the media, the US also used a diplomatic countermeasure to combat the disinformation threat. They sent delegates from the health care system to talk to Soviet health care professionals in order to convey the message that the US was not pleased with this disinformation campaign (United States Department of State 1987, 42). This did not prove to be effective. The US started to more actively pursue this line of counter measures when the story reached domestic media outlets. It was around this time that the AMWG became involved and published their report on this disinformation campaign.

Another counter measures in the Operation InfeKtion case came from the Soviet Union. Scientists in the Soviet Union did not agree with the claim that the HIV/AIDS virus could be artificially synthesized (United States Department of State 1987, 37). A prominent Soviet scientist even went as far as to debunk this claim in a public interview. He stated that

“Providing a simple answer to the question concerning the original source of the AIDS pathogen is very difficult ... as studies testify, the virus itself might have existed in nature for a long time.” (United States Department of State 1987, 37) This statement goes against the claim that the virus was recently developed in a lab. The fact that a prominent Soviet scientist openly disagreed with the claim that the virus was recently developed in a lab decreased the credibility of the information.

A factor that can be identified from this case as influential on the process of Shaping the US’ attitude towards disinformation is their level of threat perception. Before the story reached the media outlets in the US, the counter measures consisted of letting foreign media outlets know that the US did not agree with their story they were reporting. However, once the story broke in the US, the counter measures became more prominent by actively debunking the story in report and sharing these reports with the American public as well as the international community.

5.1.3. Discussion

The attitude shaping factors identified in this section are the level of education on the subject of disinformation, the actors in power and the level of threat perception. These factors have been previously discussed in sections 4.1.4 and 4.2.4. However, in the context of counter measures the following statements could be made.

Education is one of the ultimate countermeasures against disinformation. Education, especially through historical disinformation cases, leads to a better understanding of the disinformation threat which helps create more informed and therefore more effective policies. Education also helps with easier, and possibly earlier, identification of disinformation, which has been argued to be a valuable counter measure. In disinformation cases, those in power have often been the securitizing actor. As previously discussed, in securitizing an issue, the securitizing actor gains the power to use extraordinary measures. These extraordinary measures have the potential to be the missing part of the counter strategy. As for the level of threat perception, it is not surprising that counter measures are closely related to threat perception. Usually, the higher the level of threat perception, the more aggressive the counter measures. The level of threat perception influences the strategy employed, for example offensive or defensive.

5.2. Counter Measures in the Information Age

5.2.1. Government Policies on Disinformation

On a federal level the US currently has multiple governmental organizations involved in the countering of the disinformation threat. Some of these organizations have only recently been tasked with countering this threat. An example of this being the Department of Homeland Security (DHS). The DHS officially got involved in countering Russian disinformation in 2018 and created the Countering Foreign Influence Task Force (Bodine-Baron et al. 2018, 14). As of today, the DHS however does not actively get involved in counter disinformation practices. Instead they have been focusing on the coordination of "information-sharing and partnerships between state and local governments, private sector companies, and federal departments and agencies." (Bodine-Baron et al. 2018, 14) Instead of actively countering the disinformation threat, the DHS has chosen a more defensive route and has been investing in the strengthening of the disinformation targets. The Department of Justice, in support of the DHS, has been focusing on the legal aspects of countering disinformation. Through task forces such as the Cyber Digital Task Force and the Foreign Influence Task Force they investigate and report on disinformation campaigns (Bodine-Baron et al. 2018, 15). The problem with these task forces, especially the Foreign Influence Task Force, is that they only come into play when there has been a clear violation of US law (Bodine-Baron et al. 2018, 15).

The US has taken counter measures through their legislation. For example, the National Defense Authorization Act (NDAA), of which the Portman-Murphy Counter Propaganda Bill was a part, was signed into law in 2017 (Bodine-Baron et al. 2018, 16). The two Senators that introduced this bill were worried about national security because of the growing threat of Russian influence campaigns. The Senators believed the US government should be more actively involved in countering disinformation. Important to note is that no concrete actions have been taken since this bill was signed into law. The US has not been entirely defensive in their efforts to counter disinformation. As part of a larger operation to diminish the Russian threat they have imposed sanctions on Russia under the Countering America's Adversaries Through Sanctions Act (CAATSA) of 2017 (Bodine-Baron et al. 2018, 16). Most of these sanctions were of an economic nature. This act has allowed the US to increase the level of imposed sanctions on Russia when they view this to be necessary. However, many officials believed that the US has reached the maximum level of sanctions

they can impose on Russia before it starts hurting themselves or their allies (Selected Committee on Intelligence United States Senate 2019b, 43).

Since Russia's intervention into Ukraine in 2014, the international community have been employing several joined tactics that have been summarized as 'Engage, Expose and Enhance', the EEE-method, to fight disinformation (Cull et al. 2017, 72). The 'Engage' approach is aimed at reducing tensions by cultivating relationships. The 'Expose' approach "involves actively tracking this activity and publicizing it in order to make explicit the attempted manipulation of populations." (Cull et al. 2017, 72) The 'Enhance' approach is aimed at smaller media outlets. It is important to teach these local media outlets to recognize disinformation in order to prevent the spread (Cull et al. 2017, 72-73). These approaches were however not officially adopted by the US. They are being used to an extent but currently the US lacks an officially coordinated plan to deal with the disinformation security threat (Bodine-Baron et al. 2018, 13).

To summarize, one could argue that the US is building a legal framework to counter disinformation more actively. However, since this framework is not yet fully operational, they have been employing more defensive counter measures, such as investing in the strengthening of potential disinformation targets in order to minimize the damage. What this shows is that the US is aware of the threat and building towards a long-term defense against the threat instead of only immediate reactive actions.

5.2.2. Social Media Policies on Disinformation

The exposure of the fact that several social media companies were involved in the Russian meddling campaign of 2016 caused these platforms to re-evaluate their disinformation policies (Bodine-Baron et al. 2018, 17). Companies like Facebook took actions and started cleaning up the accounts that spread disinformation as well as the content they had spread. Companies like Facebook, Twitter and Google are currently better equipped to counter disinformation practices than any governmental body is (Nemr and Gangware 2019, 26). Not only do they have more resources financially, they also have algorithms in place that can track user activity on their platforms (Nemr and Gangware 2019, 26). These algorithms learn from previous confirmed disinformation cases and apply what they learned to new potential disinformation cases. Through these algorithms the companies are able to track where the information originated, who looks at it and who shares it. This provides evidence as to who is behind disinformation campaigns and who might be involved in the spread. It might

also provide valuable insights into which disinformation campaign is more effective and which factors make the campaign more effective than others.

Disinformation is profitable for these platforms in the short run. Social media platforms gain their enormous revenue from advertisements and advertisements have better results when they are sensational. Sensational advertisements are more likely to contain disinformation and therefore disinformation is profitable for these companies (Nemr and Gangware 2019, 26). However, in the long run disinformation is less profitable. When people realize that these advertisements are linked to disinformation, they are likely to lose trust in these platforms which will result in loss of income for these companies (Nemr and Gangware 2019, 27).

One of the main platforms used in the disinformation campaign of 2016 was Facebook. After this came to light, Facebook made public that they would be implementing several policies to counter the spread of disinformation (Nemr and Gangware 2019, 27). As for political advertisements, Facebook has developed a system of transparency when it comes to advertisements (Bodine-Baron et al. 2018, 18). Users can now view who issued the advertisement and who it is aimed at. Facebook has also enlisted the help fact checkers from a third party. This way they have outsourced the huge task of determining what is disinformation and what not (Nemr and Gangware 2019, 27). Next to Facebook, Russian disinformation specialists have made a lot of use of Twitter. Twitter can be seen as even more effective than Facebook in the spread of disinformation since its newsfeed is less tied to one's personal network, as is the case for Facebook (Nemr and Gangware 2019, 31). Surveys conducted on the spread of disinformation on Twitter have even stated that disinformation on Twitter reaches more people than the truth (Nemr and Gangware 2019, 31). In recent years, Twitter has also taken action to counter disinformation practices. For example, advertisements on Twitter are now labeled to show who purchased them and users are able to report them if they believe the advertisements are spreading false or inappropriate information (Nemr and Gangware 2019, 31).

To summarize, many social media companies that have been previously involved in disinformation practices have taken steps to counter it. However, in the short-run, disinformation is profitable for these companies, due to the revenue the companies earn from sensational advertising. It has been argued that at this moment, social media companies like Facebook and Twitter are better equipped to deal with the disinformation threat. In part because they have more financial resources but also because they have algorithms in place

which obtain information from every confirmed disinformation case and apply it to other potential disinformation campaigns in order to determine their legitimacy.

5.2.3. United States Presidential Elections of 2016

It was in the second half of 2016, that US government officials first realized that the Russians were running an influence campaign on the Presidential Elections. At the time they believed to be up against an entirely new kind of threat, however, their information on the scope of the threat was incomplete (Selected Committee on Intelligence United States Senate 2019b, 3). When they learned about the Russian interference, the first response of the US was to issue a warning against Russia. These warnings were given before the elections took place but seemed to have little to no effect on Russian efforts to influence the elections (Selected Committee on Intelligence United States Senate 2019b, 3). The administration at that time has said to have issued at least five warnings to different levels of the Russian government (Selected Committee on Intelligence United States Senate 2019b, 25). These warnings however, were constrained due to the fact that the US did not want to give the American public the feeling they lost control of the elections, because that would play exactly into the Russian plan (Selected Committee on Intelligence United States Senate 2019b, 4). They were also concerned that warning to the public would be interpreted as the administrations favoring one candidate over the other (Selected Committee on Intelligence United States Senate 2019b, 17). Lastly, they were concerned that when they imposed punitive sanctions on Russia, the Russians would only undertake even more disinformation campaigns against the US (Selected Committee on Intelligence United States Senate 2019b, 36).

Before the elections actually took place, the US tried to combat the Russian disinformation campaign through the diplomatic route, by asking them nicely to stop. After the elections, when it became clear that the Russians had not discontinued their disinformation practices, the US took sterner measures. They took economic sanctions against Russia as well as political sanctions which included the shuttering of Russian diplomatic facilities in the US and expelling Russian government personnel (Selected Committee on Intelligence United States Senate 2019b, 3). These measures did not have the desired effect, the Russians kept their disinformation operations going. What followed can best be described as confusion within the American government.

At the basis of that confusion was the fact that most government officials had little to no understanding of what they were dealing with exactly. This lack of understanding led to an

inability to respond quickly and adequately to the threat of electoral interference. The argument that these government officials did not have a sufficient understanding of the threat can be traced back to the fact that the Obama administration constrained the information flow to these officials with regards to the electoral interference and disinformation. Briefings on the Russian disinformation campaign were only given to a select small group of government officials and reports were often given verbally instead of in written form (Selected Committee on Intelligence United States Senate 2019b, 13). This meant that only a select group of people was aware of what was going on. This group unfortunately did not have all the power needed to effectively counter the threat. If more government officials would have been involved, as well as the intelligence committee, policy options could have been debated and discussed in order to be successful in their fight against Russian disinformation (Selected Committee on Intelligence United States Senate 2019b, 50). This lack of widespread involvement led to an inability to form adequate policy options within the limited time frame. What one can take away from this example is that the US was led in their counter measures by fear. Most of their decisions on what to do, or more specifically, what not to do, were al based on the fear of hurting themselves or their allies.

5.2.4. Discussion

The attitude shaping factors identified in this section are the legal framework, social media policies, the level of understanding of the problem and the level of fear. Not often specifically mentioned in literature, but very important is the level of fear experienced by the US. The level of fear ties into threat perception, which as stated before, has been often discussed. Fear determines the level of threat perception which in turn determines the counter strategy.

The legal framework in the US is not often discussed in the literature, it is mostly just briefly mentioned. This is interesting since one would benefit from a deeper understanding of the current legal framework. A better understanding of the framework allows one to place counter measures into perspective and possibly identify the legal shortcomings with regards to these counter measures. Since the legal framework largely determines the extent of the counter measures and thus the attitude of the US, research into the legal framework, its shortcomings and its strengths, is important.

The literature often looks at the effects of social media on disinformation. It has been determined that in the information age social media is the main tool with which

disinformation is spread. Social media policies affect the attitude of a nation since a very large percentage of the population has one or more social media accounts. Non-government actors like social media companies are becoming an increasingly important factor in the disinformation issue. Both in countering disinformation as well as spreading it. In many social media disinformation cases, the government does not have the power to act on it. Social media companies, however, do have the power to take the measures they see fit. Therefore, the government has increasingly had to hand over power to social media companies in their fight against disinformation. Another important aspect of social media companies is that they learn from past disinformation cases. Most platforms have algorithms in place which once a disinformation case has been detected learn from it in order to apply that knowledge to detect future disinformation cases. These algorithms have proven to be very effective and illustrate the importance of learning from past disinformation cases.

5.3. Conclusion

The first section of this chapter analyzed the counter measures in the Cold War. In the Cold War, most counter measures were defensive in nature, debunking disinformation and increasing awareness as illustrated by Operation InfeKtion. In the information age counter measures were still mainly defensive in nature, debunking disinformation and increasing public awareness. In the information age, the US also prepared for more offensive measures by building a legal framework to be used in disinformation cases. Another important actor in the fight against disinformation in the information age are social media companies. These companies offer the platform used to spread disinformation and are therefore continuously developing new counter measures through learning from past cases. This section ended with the analysis of the case of the 2016 presidential elections, which showed that the US issued warnings and imposed economic sanctions on Russia for their interference in the elections.

None of the counter measures taken by the US seemed to have impacted the amount of disinformation campaigns coming from Russia. Many of the counter measures were defensive in nature. These measures were aimed at increasing public awareness through publicly exposing and debunking disinformation campaigns. In the Cold War, this method was given the name RAP method. In the information age, this method was more commonly known as the EEE method. Both methods are effective in regard to spreading public awareness and discrediting disinformation campaigns as well as discrediting those spreading it. However, due to the vast amount of disinformation campaigns and the time it takes to properly refute

these campaigns, these methods are not enough. In the Cold War, government policies first followed a defensive strategy, this later changed towards more offensive with the establishment of for example, the AMWG. In the information age, government officials did not always get the chance to be able to understand. During the 2016 elections, only a select group of people was kept informed on any Russian interference. In this time period, social media companies were better equipped to deal with the disinformation threat due to their financial situation as well as algorithms that were able to learn from previous disinformation cases in order to detect new ones.

As for the factors that shaped the US' attitude towards disinformation one could state that the counter measures are determined by those who hold power, education on the subject and the level of threat perception within the US. Factors such as fear, the legal framework and social media policies can also be identified as influential in this process of attitude formation. What these factors have shown is that in order to develop effective counter measures, more research needs to be conducted. Especially in the information age, where governments in the disinformation issue are slowly being replaced by non-government actors, education on all levels is extremely important. One of the ways in which a better education can be achieved is by looking at the history of disinformation.

6. Comparison and Recommendation

In this chapter, the findings of the analysis performed in the previous two chapters will be compared in order to determine any similarities and differences between the time periods. These similarities and differences might prove important for the US in determining which attitude to adopt in future when it comes to the disinformation threat. The first section will highlight the differences and similarities in threat perception between the two time periods. The second section will do the same for counter measures. In the end, a policy recommendation will be given.

6.1. Threat Perception

The analysis of threat perceptions dealt with both active measures and disinformation. Throughout the analysis it became clear that since disinformation is a part of active measures, many answers to the guiding questions were similar. In both time periods, the US was mainly focused on the Russians being behind the disinformation threat since most of the disinformation practices benefitted Russian interests. The difference between the referent subjects of both time periods is that in the Cold War, the documents clearly blamed Russia by using Russian translations of key concepts and the argument that disinformation only seemed to benefit Russian objectives. In the information age, placing blame on Russia was less simple due to the use of third parties. Now the US had to prove that non-government actors such as the IRA were affiliated with the Kremlin.

The aim of the active measure campaigns remained roughly the same throughout the years. In both time periods, the aim was to bring down the US while simultaneously lifting Russia up. More specifically, exploit already existing tensions within the US in order to destabilize and weaken the country.

The one obvious difference between the Cold War and the information age is the technological advancements. Throughout the years, Russia has changed their disinformation tactics to most efficiently make use of new technologies. Technological advancements such as the internet allowed for an increase in the number of disinformation campaigns as well as the speed and size with which they are being disseminated. Another difference is the shift in focus from the threat to national security to the threat to the individual. Although the US still sees disinformation as a threat to national security, they are now realizing that the disinformation campaigns targeted at smaller groups within society or individuals are what is causing the threat to national security.

As for the specific case studies, the aim of the disinformation campaign is roughly the same. Both campaigns aim to weaken the position of the US in the international community. However, the disinformation campaign surrounding the 2016 Presidential Elections had the additional aim to elect a US president that was more favorable to Russia providing Russia with more influence on American politics. In both cases, Russia used already existing tensions to increase the effectiveness of their disinformation campaign. In the Cold War this meant exploiting both racial and military tensions, whereas in the information age the campaign was focused on exploiting political tensions. The military tensions exploited in the Cold War case explicitly played on international tensions in the aftermath of World War II, whereas in the information age the focus was on exacerbating internal tensions within the US.

The main attitude shaping factors identified throughout the Cold War are the US government as the securitizing actor, the influence of subgroups on society, threat perception, and successful, large-scale disinformation operations such as Operation InfeKtion. In the information age, the factors identified are the level of unity, the level of understanding and the estimate made by the US on the capabilities, intentions and willingness of Russia to launch these disinformation campaigns against them. Most of these factors have at least partially been discussed in the current literature, however, some, like the estimates on willingness and capabilities, as well as large disinformation cases have not been researched to the extent that they have attributed to a significantly better understanding of the problem. Most factors identified seem to have a political nature and are policy oriented. One could argue that since large-scale disinformation campaigns like Operation InfeKtion were influential in the attitude shaping process in the Cold War, they should have been influential in the information age as well. However, it seems the US does not look at history when it comes to new disinformation cases, or at least not enough to learn from these previous cases in order to decrease their vulnerability.

6.2. Counter Measures

The analysis on counter measures looked at government policies, specific methods to counter disinformation and, in the case of the information age, the policies of social media companies. A similarity between the time periods can be found in the fact that they both seem to transition from mainly defensive policies on disinformation towards more offensive policies. From the Cold War to the information age, policies such as détente are slowly being

replaced by a legal structure that allows the US to take actions against disinformation operations and the perpetrator behind these operations.

Since the way in which disinformation is disseminated changed a lot from the Cold War to the information age, the counter measures have undergone some changes as well. The goal of the counter measures to expose disinformation is still one of the main aspects. In both the RAP method and the EEE method, focus is put on exposing disinformation campaigns in a structured and well substantiated manner. The aim of exposing these disinformation campaigns is to increase public awareness of the threat. In the information age, more effort was put in increasing public awareness through the method section called 'Enhance'.

In the Cold War, the US' main focus was on countering disinformation through their foreign policies, whereas in the information age, they shifted their focus to include more legal options to counter disinformation. This shift could be explained by the increase of the involvement of non-state actors on which foreign policy has less of an effect. These non-state actors are mostly social media companies. These platforms have been developing their own measures to counter disinformation that seem to be more effective than government policies and have become a shaping factor of the US attitude. This can be explained by the difference in funding between the government and private companies.

As for the case studies, in both cases the counter measures taken did not have the desired effect. In both cases, the ones involved did not have enough knowledge about the threat and disinformation in general to design and implement effective counter measures. In the case of Operation InfeKtion most counter measures were reactive in nature, such as debunking the story through scientific evidence and threatening diplomatic actions if the Soviet Union did not stop their disinformation practices. In the case of the 2016 elections, the US had to deal with multiple disinformation stories leading up to the elections. This longer time period allowed them to impose sanctions on Russia in order to get them to stop their disinformation campaign. Russia, however, did not respond to these sanctions as the US would have hoped. The US, however, chose not to react with firmer measures due to fear of hurting themselves or their allies.

The main attitude shaping factors identified throughout the Cold War are the securitizing actor, the level of education and threat perception. In the information age, the factors identified are the lack of understanding of disinformation, the legal framework, social media policies, and the level of fear. As with threat perception, the lack of understanding disinformation remains a shaping factor in the information age. As previously mentioned, one could argue that in order to effectively counter disinformation, one should focus on attitude

shaping factors in historical cases in order to determine which parts of the attitude were effective and which were not. The results of this analysis could prove crucial in countering future disinformation cases.

6.3. Policy Recommendation

The US policy with regard to disinformation started a period of change in the wake of the 2016 Presidential Elections (Ingram 2020, 9). At the basis of this change lies the State Department's Global Engagement Center (GEC) which can be seen as the main coordinating mechanism in the battle against disinformation (Ingram 2020, 2). Currently, the US is building a legal framework which allows the GEC to serve as "a "force multiplier" of a broader U.S. government effort via not only coordination and looking for opportunities to drive innovation across a "system of systems" but identifying and plugging gaps." (Ingram 2020, 11) The efficiency and effectiveness of the GEC depends on several factors, one of which has become apparent throughout this research. This factor is the need to learn from history. The main policy recommendation this thesis highlights is the need for a better understanding of the disinformation threat by taking a history-oriented approach to policy. These lessons can be drawn, for example, from the history of the institutions involved (Ingram 2020, 2), from historical disinformation cases, or from defectors that have worked in this industry. A history-oriented approach to policy allows for a better understanding of disinformation among the professionals that deal with disinformation, both governmental and non-governmental. Which in turn allows for better informed decisions when it comes to a counter strategy as well as the ability to potentially identify disinformation in an earlier state limiting the damage it can do. Practical ways in which this can be achieved is by organizing seminars for professionals dealing with disinformation. These seminars could be given by other professionals that have more knowledge on the subject or by defectors that have previously been employed in the disinformation field. As for the rest of the population, education on disinformation should become part of history lessons given in school. This way familiarization with disinformation starts from a young age, which will create a critical mindset which decreases the potential of falling for a disinformation campaign.

7. Conclusion

This thesis set out to answer the question "*What factors shaped the United States' attitude towards Russian disinformation during Operation InfeKtion (1980s) and the Russian influence campaign in the United States in 2016 and how can the differences and similarities between these time periods be explained?"* This question aimed to historicize the main questions in the disinformation literature, how does one identify disinformation and how does one counter it? The answer to the research question was obtained through analyzing US government documents. These documents were analyzed through the lens of securitization theory which provided the guiding questions used.

The first analytical chapter was focused on threat perception in the US. The main attitude shaping factors identified throughout this chapter were the securitizing actor, the influence of subgroups on society, threat perception, successful, large-scale disinformation operations such as Operation InfeKtion, the level of unity and the estimate made by the US on the capabilities, intentions and willingness of Russia. Most of these factors had been previously discussed in the literature, all to a different extent. The differing levels of research on these factors highlighted the lack of understanding and knowledge on some crucial aspects of the disinformation threat. What these factors illustrated is that in their perception of the disinformation threat, the US is mostly policy oriented thereby largely ignoring the history of disinformation. They sometimes seem to forget that disinformation is not a new threat and that they could look at historical cases to learn from it.

The second analytical chapter was focused on the counter measures taken by the US in both time periods. Due to technological advancements there was a significant change in the way disinformation campaigns were conducted. This resulted in a need for changed counter measures as well. In the Cold War, counter measures were almost solely the responsibility of the governing body, however, in the information age, part of this responsibility was taken on by social media companies who had become the main platform used to share disinformation. The main attitude shaping factors identified throughout analyzing the counter measures were the securitizing actor, threat perception, the lack of understanding of disinformation, the legal framework, social media policies and the level of fear. What these factors show is that that there is a need to educate the US on disinformation. A better understanding of disinformation allows for a more accurate threat perception and allows for a better set of counter measures to be taken without the fear of harming the US or its allies. In order to learn more about disinformation, it is crucial to look at historical cases.

To conclude, this thesis' main argument is that the US in their encounters with disinformation has been more policy oriented, where one could argue that a historical approach would have been more beneficial. Just as social media algorithms learn from past disinformation cases in order to identify future ones, the US should aim to learn from past disinformation cases. Studying the methods used can provide valuable information for detecting disinformation cases in an earlier stage and studying the effectiveness of previous counter measures could prove helpful in creating counter measures in the present. Not only would this be beneficial for the US government, creating a better understanding of disinformation among the public could decrease the public's vulnerability to the threat. This increased level of understanding and awareness among the government and the public will most likely result in a higher sense of security.

This research has shown that more research into the history of disinformation is required. Possible avenues of further research could be into identifying factors that characterize disinformation in order to be able to pick up disinformation in its early stages. Another possible research avenue identified in this thesis could be into who carries the responsibility for countering the disinformation threat. Due to the rise of private companies, their growing involvement in disinformation and their increasing financial abilities, it is interesting to look at who assigns and takes responsibility for countering the disinformation threat. One more research possibility that could be an addition to this research is to apply this or a similar research question to other cases. Russia is not the only nation attacking the US with disinformation activities and the US is not the only nation being threatened by disinformation. As for current US policy with regards to disinformation this thesis recommends that in order to increase the effectiveness of the current policies, both professionals in the field as well as the population should be educated on disinformation from an historical perspective. This can be done through seminars as well as the inclusion of disinformation lessons in the school curriculum.

Bibliography

Andersson, Jan Joel. 2015. “Hybrid Operations: Lessons from the Past.” https://www.jstor.org/stable/resrep06843.

Araźna, Marzena. 2015. “CONFLICTS OF THE 21ST CENTURY BASED ON MULTIDIMENSIONAL WARFARE– ‘HYBRID WARFARE’, DISINFORMATION AND MANIPULATION.” *Security and Defence Quarterly* 8 (3): 103–29. https://doi.org/10.5604/23008741.1189421.

Balzacq, Thierry, Sarah Léonard, and Jan Ruzicka. 2016. “‘Securitization’ Revisited: Theory and Cases.” *International Relations* 30 (4): 494–531. https://doi.org/10.1177/0047117815596590.

Banjo, Shelly. 2019. “Facebook, Twitter and the Digital Disinformation Mess.” *The Washington Post*, October 2, 2019.

Batyuk, Vladimir I. 2017. “The US Concept and Practice of Hybrid Warfare.” *Strategic Analysis* 41 (5): 464–77. https://doi.org/10.1080/09700161.2017.1343235.

Baudet, Floribert, Eleni Braat, Jeoffrey van Woensel, and Aad Wever. 2017. *Perspectives on Military Intelligence from the First World War to Mali*. Springer.

Beisner, Robert L. 2006. *Dean Acheson : A Life in the Cold War*. Oxford: Oxford University Press.

Bennett, W. Lance, and Steven Livingston. 2018. “The Disinformation Order: Disruptive Communication and the Decline of Democratic Institutions.” *European Journal of Communication* 33 (2): 122–39. https://doi.org/10.1177/0267323118760317.

Bittman, Ladislav. 1985. *The KGB and Soviet Disinformation. An Insider’s View*. Washington.

Bodine-Baron, Elizabeth, Todd C. Helmus, Andrew Radin, and Elina Treyger. 2018. “Countering Russian Social Media Influence.” Santa Monica, CA.

Boghardt, Thomas. 2009. “Soviet Bloc Intelligence and Its AIDS Disinformation Campaign.” *Studies in Intelligence* 53 (4): 1–24. https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol53no4/pdf/U- Boghardt-AIDS-Made in the USA-17Dec.pdf.

Bruce, James B., and Michael Bennett. 2014. “No Foreign Denial and Deception: Analytic Imperatives.” In *Analyzing Intelligence : National Security Practitioners’ Perspectives*, 197–214. Washington, D.C.: Georgetown University Press.

Brunner, Edward. 2010. “How Can I Tell My Grandchildren What I Did in the Cold War?” In *Pressing the Fight : Print, Propaganda, and the Cold War*, edited by Catherine Turner and Greg Barnhisel, 169–92. Amherst: University of Massachusetts Press.

Chandra, Satish, and Rahul Bhonsle. 2015. “National Security: Concept, Measurement and Management.” *Strategic Analysis* 39 (4): 337–59.

Cheyfitz, Eric. 2017. *The Disinformation Age: The Collapse of Liberal Democracy in the United States*. *The Disinformation Age: The Collapse of Liberal Democracy in the United States*. New York: Routledge. https://doi.org/10.4324/9781315222837.

Cooke, Nicole A. 2017. “Posttruth, Truthiness, and Alternative Facts: Information Behavior and Critical Information Consumption for a New Age.” *Library Quarterly* 87 (3): 211–21. https://doi.org/10.1086/692298.

Cull, Nicholas J., Vasily Gatov, Peter Pomerantsev, Anne Applebaum, and Alistair Shawcross. 2017. “Soviet Subversion, Disinformation and Propaganda: How the West Fought Against It An Analytic History, with Lessons for the Present.” London. http://www.lse.ac.uk/iga/assets/documents/arena/2018/Jigsaw-Soviet-Subversion-Disinformation-and-Propaganda-Final-Report.pdf.

Department of State. 1950. “NSC-68.”

Ellick, Adam B., and Adam Westbrook. n.d. *Operation Infektion. Russian Disinformation: From Cold War to Kanye*. The New York Times. https://www.nytimes.com/2018/11/12/opinion/russia-meddling-disinformation-fake-news-elections.html.

Gaddis, John Lewis. 2000. *The United States and the Origins of the Cold War, 1941-1947. The Public Historian*. New York: Columbia University Press.

———. 2005. *Strategies of Containment : A Critical Appraisal of American National Security Policy During the Cold War*. New York: Oxford University Press.

Garthoff, Raymond L. 2004. "Foreign Intelligence and the Historiography of the Cold War." *Journal of Cold War Studies* 6 (2): 21–56. https://doi.org/10.1162/152039704773254759.

Gerrits, André W.M. 2018. "Disinformation in International Relations: How Important Is It?" *Security and Human Rights* 29 (1–4): 3–23. https://doi.org/10.1163/18750230-02901007.

Global Engagement Center. 2020. "Pillars of Russia's Disinformation and Propaganda Ecosystem."

Gromyko, Alexey. 2015. "Russia-EU Relations at a Crossroads: Preventing a New Cold War in a Polycentric World." *Southeast European and Black Sea Studies* 15 (2): 141–49. https://doi.org/10.1080/14683857.2015.1060018.

Hendricks, Vincent F., and Mads Vestergaard. 2019. *Reality Lost: Markets of Attention, Misinformation and Manipulation*. *Reality Lost: Markets of Attention, Misinformation and Manipulation*. Springer International Publishing. https://doi.org/10.1007/978-3-030-00813-0.

Ingram, HJ. 2020. "PERSUADE OR PERISH Addressing Gaps in the U.S. Posture to Confront Propaganda and Disinformation Threats." George Washington University.

Jeansonne, Glen, and David Luhrssen. 2014. *War on the Silver Screen : Shaping America's Perception of History*. Lincoln: University of Nebraska Press.

Jones, Seth G. 2018. "Going on the Offensive: A U.S. Strategy to Combat Russian Information Warfare."

Kaminska, Izabella. 2017. "A Lesson in Fake News from the Info-Wars of Ancient Rome." *Financial Times*, January 17, 2017. https://www.ft.com/content/aaf2bb08-dca2-11e6-86ac-f253db7791c6.

Kaplan, Jeffrey. 2019. "Introduction." *Terrorism and Political Violence* 31 (1): 1–8. https://doi.org/10.1080/09546553.2018.1542877.

Lanoszka, Alexander. 2019. "Disinformation in International Politics." *European Journal of International Security*, 1–22. https://doi.org/10.1017/eis.2019.6.

MacDonald, Eve. 2017. "The Fake News That Sealed the Fate of Antony and Cleopatra." The Conversation. 2017. https://theconversation.com/the-fake-news-that-sealed-the-fate-of-antony-and-cleopatra-71287.

Matz, Johan. 2016. "'All Signs Indicate That Gestapo Agents Murdered Him': Soviet Disinformation, the Katyn Massacre and the Raoul Wallenberg Case, 1945-7." *International History Review* 38 (1): 148–73. https://doi.org/10.1080/07075332.2015.1016994.

McMahon, Robert J. 2009. *Dean Acheson and the Creation of an American World Order*. Washington, D.C.: University of Nebraska Press.

Mesch, Gustavo, and Ilan Talmud. 2010. *Wired Youth: The Social World of Adolescence in the Information Age*. *Wired Youth: The Social World of Adolescence in the Information Age*. London: Routledge. https://doi.org/10.4324/9780203855102.

Nemr, Christina, and William Gangware. 2019. "WEAPONS OF MASS DISTRACTION: Foreign State-Sponsored Disinformation in the Digital Age." https://www.state.gov/wp-content/uploads/2019/05/Weapons-of-Mass-Distraction-Foreign-State-Sponsored-

Disinformation-in-the-Digital-Age.pdf.
Posetti, Julie, and Alice Matthews. 2018. “A Short Guide to the History of ’fake News’ and Disinformation.” *ICFJ (International Center for Journalists)*. https://doi.org/10.1207/s15327728jmme1502_3.
Pynnöniemi, Katri. 2019. “The Asymmetric Approach in Russian Security Strategy: Implications for the Nordic Countries.” *Terrorism and Political Violence* 31 (1): 154–67. https://doi.org/10.1080/09546553.2018.1555995.
Ramrattan, Lall B., and Michael Szenberg. 2017. “American Exceptionalism: An Appraisal—Political, Economic, Qualitative, and Quantitative.” *The American Economist* 62 (2): 222–46. https://doi.org/10.1177/0569434516672793.
Reiss, Megan. 2019. “Disinformation in the Reagan Years and Lessons for Today.” www.jstor.org/stable/resrep19125.
Rid, Thomas. 2020. *Active Measures. The Secret History of Disinformation and Political Warfare*. London: Profile Books.
Schiffrin, Anya. 2016. “DISINFORMATION AND DEMOCRACY: THE INTERNET TRANSFORMED PROTEST BUT DID NOT IMPROVE DEMOCRACY.” *Journal of International Affairs* 71 (1): 117–25.
Schoen, Fletcher, and Christopher Lamb. 2012. “Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference.” *INSS Strategic Perspectives* 11. https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/inss/Strategic-Perspectives-11.pdf.
Scott, Kenneth. 1929. “Octavian’s Propaganda and Antony’s De Sua Ebrietate.” *Classical Philology* 24 (2): 133–41. https://doi.org/10.1086/361116.
Selected Committee on Intelligence United States Senate. 2019a. “RUSSIAN ACTIVE MEASURES CAMPAIGNS AND INTERFERENCE IN THE 2016 U.S. ELECTION VOLUME 2: RUSSIA’S USE OF SOCIAL MEDIA WITH ADDITIONAL VIEWS.”
———. 2019b. “RUSSIAN ACTIVE MEASURES CAMPAIGNS AND INTERFERENCE IN THE 2016 U.S. ELECTION VOLUME 3: U.S. GOVERNMENT RESPONSE TO RUSSIAN ACTIVITIES.”
Smith, Timothy J. 2014. “Overlord/Bodyguard: Intelligence Failure through Adversary Deception.” *International Journal of Intelligence and CounterIntelligence* 27 (3): 550–68.
Soma, Katrine, Catrien J.A.M. Termeer, and Paul Opdam. 2016. “Informational Governance - A Systematic Literature Review of Governance for Sustainability in the Information Age.” *Environmental Science and Policy* 56: 89–99. https://doi.org/10.1016/j.envsci.2015.11.006.
Tari, Berna. 2011. “Discourse Analysis.” In *Encyclopedia of Consumer Culture*, 461–63. SAGE Publications.
Taureck, Rita. 2006. “Securitization Theory and Securitization Studies.” *Journal of International Relations and Development* 9 (1): 53–61. https://doi.org/10.1057/palgrave.jird.1800072.
Taylor, Philip M. 2003. “The Gutenberg Galaxy.” In *Munitions of the Mind : A History of Propaganda*, 87–88. Manchester: Manchester University Press.
The DFRLab Team. 2019. “OPERATION ‘SECONDARY INFEKTION’: A SUSPECTED RUSSIAN INTELLIGENCE OPERATION TARGETING EUROPE AND THE UNITED STATES.”
The Project Gutenberg eBook. 2005. “The Art of War, by Sun Tzu.” The Project Gutenberg EBook. 2005. https://www.utoledo.edu/rotc/pdfs/the_art_of_war.pdf.
Tutui, Viorel. 2017. “Some Reflections Concerning the Problem of Defining Propaganda.”

Argumentum: Journal of the Seminar of Discursive Logic, Argumentation Theory and Rhetoric 15 (2): 110–25.

TVB. 2019. “National Television Penetration Trends TOTAL & TV HOUSEHOLDS.” 2019.

Tzu, Sun, and Lionel Giles. 1994. *Sun Tzu On The Art Of War*. https://doi.org/10.4324/9781315030081.

United States Department of State. 1987. “Soviet Influence Activities: A Report on Active Measures and Propaganda, 1986 - 87.”

Wæver, Ole. 1995. “Securitisation and Desecuritisation.” In *On Security*, edited by Ronnie D Lipschutz. https://www.libraryofsocialscience.com/assets/pdf/Waever-Securitization.pdf.

Walton, Calder. 2019. “Spies, Election Meddling, and Disinformation: Past and Present.” *The Brown Journal of World Affairs* 26 (1): 107–24.

Whitton, John B. 1951. “Cold War Propaganda.” *The American Journal of International Law* 45 (1): 151–53. https://doi.org/10.2307/2194791.

Young, C.W. Bill, and Federal Bureau of Investigation. 1987. “Congressional Record - Extensions of Remarks: Soviet Active Measures in the United States - An Updated Report by the FBI.”