The transformation of disinformation in cyberspace

Stoop, Arthur

The transformation of disinformation in cyberspace

Executive Master Cyber Security, Thesis

Universiteit Leiden

Executive Master Cyber Security 2021/2023

Name:	A.R. Stoop MA
Student number:	S3127532
Date of submission:	January 20, 2023
Date of defense:	January 27, 2023
First supervisor:	Prof.dr. B. van den Berg
Second supervisor:	Dr. T. van Steen

Table of Contents

Chapter 1 Introduction

During the 2018 US Midterm Elections US Cyber Command (US CYBERCOM) took the notorious Russian Troll Farm offline for interfering and sowing distrust in the elections via various disinformation campaigns (Nakashima 2019). It was the first time US CYBERCOM executed an overseas offensive cyber operation (Barnes 2018). Although it seemed that this came out of the blue, there were a whole series of events before this moment.

1.1 The problem statement and aim of this research

Propaganda and disinformation are not new concepts (Taylor 2003: 6, Rid 2020: 6-7). With the ongoing digitalization of modern society, these concepts have made their way into cyberspace. A significant disinformation campaign in contemporary history is Russia's disinformation campaigns against the United States and its federal elections. This campaign is part of the academic debate on disinformation. However, most coverage in the academic debate focuses on the events themselves and lacks a reconstruction of the transformation of disinformation into and within cyberspace, and what were the reactions is missing. Studies on disinformation appear to be snapshots instead painting the full picture (Rogers & Niederer 2019: 9).

The absence of a description of the full timeline starting even before the digitization of modern society can potentially lead to a limited understanding of disinformation and perhaps misunderstanding. A parallel can be drawn between snapshots of disinformation events and the story in Idries Shah's book *The Elephant in the Dark* (Shah 1974). In this book, a group of blind men encounters an elephant and each individual feels a different part of the elephant's body and then describes it. Their perception of what they perceive as an elephant differs so much from each other's description that they think the others are lying. As a result, they start to fight each other over their views which they believe are correct.

1.2 Research question and sub-questions

Disinformation is as old as mankind. However, we used to call it propaganda. With the rise of society's digitalization, propaganda made its way into the digitalized world (Rid 2020: 6). The use of disinformation did not start with nation-states. It started with various groups and non-state organizations that used the internet for their propaganda activities (Theohary & Rollins 2011, Whine 1999). Eventually, Russia used its Internet Research Agency for large-scale disinformation campaigns against the United States Presidential Election in 2016 (Rid 2020: 400). The Russian activities were the start of a new era of foreign influence operations where disinformation was used as an instrument of power in the international arena. Russia's aim was to spread distrust towards the political system of the United States (Rid 2020: 400).

With the rise of cyberspace, new manifestations of disinformation have appeared. These manifestations are similar to the era before the use of cyberspace, but they are also fundamentally different. This is the consequence of some of the core characteristics of how information is composed, shared, and received in cyberspace. Moreover, the way disinformation was used, is being perceived, and is being responded to has changed significantly since its large-scale dissemination over the internet, roughly since 2000. This thesis charts that development. The central research question of this thesis is:

How has the deployment, perception, and mitigation of disinformation in cyberspace changed between 2000 and 2021?

The central research question will be broken down into four sub-questions:

1 *What is disinformation, and how does it differ from propaganda used outside cyberspace?*
2 *Which phases can be distinguished in the history of disinformation in cyberspace?*
3 *How is disinformation deployed in each phase, how is it perceived, and which attempts are made to mitigate the impact of disinformation?*
4 *What lessons can be learned for the future in addressing disinformation in cyberspace?*

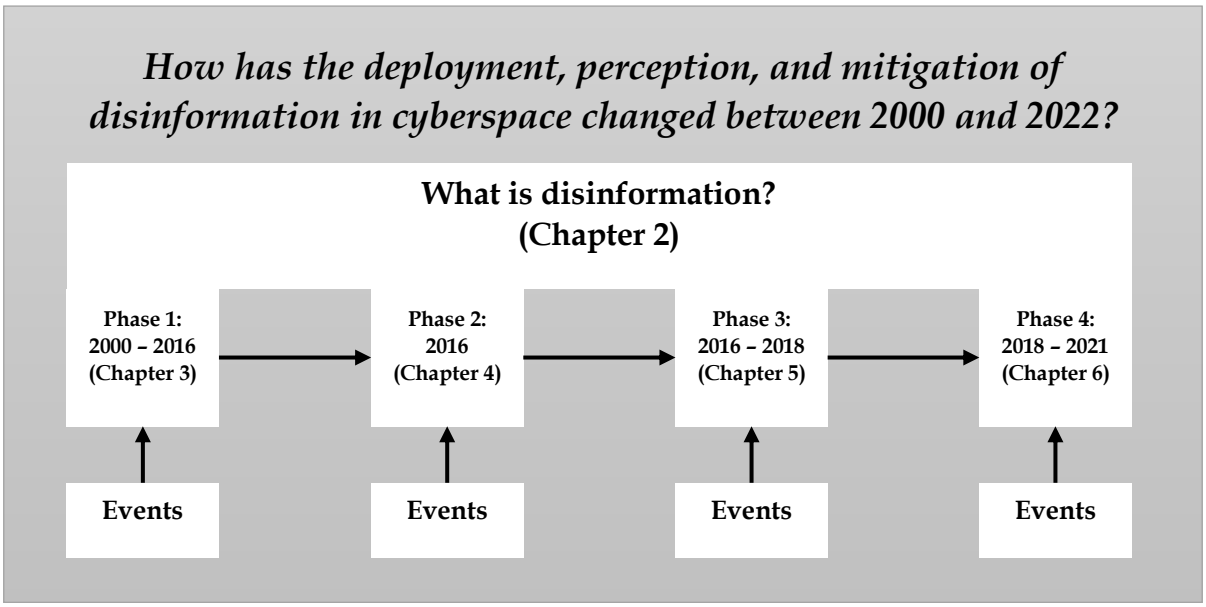
Based on a literature study, this thesis posits that the history of disinformation in cyberspace can be divided into the following phases:

- The first use of cyberspace for disinformation activities started in the early 2000s;
- The first manifestation of state-sponsored disinformation campaigns which took place during the 2016 US Presidential Election;
- The period between the 2016 US Presidential Election and the 2018 US Midterm Elections in which the United States was aware of the misuse of cyberspace by foreign adversaries for disinformation campaigns and was prepared to counter it;
- The period after the 2018 Midterm Elections where disinformation manifests itself in an uncontrolled manner and had its effects is the physical world.

1.3 Research design

This research starts with a theoretical framework on disinformation and continues to follow the chronological order of events per chapter. Each phase distinguishes itself from the previous phase since the events that took place build knowledge on the subject. This knowledge was implemented via policies and determined possible actions and the allowed responses to those actions.

Sub-question 1 will be addressed in chapter 2. Sub-question 2 will be addressed in chapter 3, chapter 4, chapter 5, and chapter 6. Sub-question 3 will be addressed in chapter 3, chapter 4, chapter 5, and chapter 6. The final sub-question, sub-question 4, will be discussed in chapter 7.



1.4 Demarcation and methodology

The United States and its advisory Russia were at the forefront of state-sponsored disinformation operations. Russia's disinformation campaign during the 2016 US Presidential Election revealed not only the extent to which information and communications technologies are being used to undermine democratic processes but also the absence of adequate protective measures (Brattberg & Maurer 2018). Russia started its disinformation campaign in 2014 against Ukraine during the conflict in Eastern Ukraine and later shifted its focus toward the United States (Lanoszka 2019: 227, Baumann 2020: 288-289). The difference between the campaign against Ukraine and the United States is that the first was part of Russia's hybrid warfare operations in the Crimea region (Splidsboel Hansen 2017: 4). The latter was not part of an armed conflict, but it was an operation in itself to spread distrust towards the political system of the United States (Rid 2020: 400). It seems to be that the disinformation campaign of 2016 against the United States was the first manifestation of a foreign influence campaign outside of hybrid warfare where disinformation was being used as an instrument of power.

Concerns over foreign disinformation campaigns have intensified after the 2016 US Presidential Election (Lanoszka 2019: 227). To counter this concern, countries like Finland and the United Kingdom based their policies on the lessons learned in the United States after the 2016 Presidential Election (Schia & Gjesvik 2020: 420-421). After the 2016 US Presidential Election at least seventeen countries experienced disinformation during their elections (Tenove 2020: 518). However, it appears that disinformation campaigns in these other countries did not manifest as in the United States. In fact, the next federal election in the United States, the 2018 Midterm Elections, was also targeted by Russia's disinformation campaign (Barnes 2018).

1.4.1 Demarcation of the research

This research is bound both by time and geography. The first manifestation of a foreign disinformation campaign to sow distrust in the targeted country was during the 2016 US Presidential Elections (Rid 2020: 400). To understand how disinformation made its way into cyberspace, the years before this election will be examined starting in the early 2000s when disinformation made its way into the digital world. The research will end with the 2020 US Presidential Election and its aftermath including the storming of the US Capitol on January 6, 2021, by protesters who did not believe that the US 2020 Presidential Election was fair and honest. This outcome in the physical and tangible world was the result of the uncontrolled manifestation of years of intensive state-sponsored disinformation campaigns. Geographically, this research will focus on the United States and Russia since they were involved in these disinformation events.

1.4.2 Research methodology

This thesis uses literature research based on a wide variety of sources for its findings and analysis. The technique used for this literature research is the snowballing technique. The starting point is a book by Thomas Rid called *Active Measures: The secret history of disinformation and political warfare* (2020). The sources of Rid are analyzed, and those sources are analyzed as well. This process was repeated until no new insights were presented.

This research starts when disinformation made its first appearance in cyberspace. Disinformation in cyberspace was a new phenomenon aimed at the information itself. Traditionally, the focus on securing cyberspace was on securing the information, maintaining the integrity of information, and keeping systems and digitalized processes available. Understanding the absence of focus on the information itself will bring further understanding of the successes of the disinformation campaigns.

The first manifestation of disinformation took place during the 2016 US Presidential Election and gave the US government new insights. Those insights have led to new policy documents, and new policies allowed new events. These new events gave new insights, and new insights led to new policies. These new policies allowed new events. This ongoing cycle repeated itself constantly. Since the Russian disinformation campaign targeted the US federal elections, federal policies were analyzed during this research to determine the gained insights and lessons implemented for the United States.

News journals are an addition to the academic sources and were, predominately, used for the reconstruction of the most contemporary events. In addition to official policy documents and news sources, federal indictments and federal congressional hearings were analyzed to reconstruct the events and actions.

The disinformation campaign against the United States was initiated and executed by Russia. For this reason, disinformation will be considered from a state-sponsored perspective where a state has a certain desired outcome. In this case, to sow distrust towards the candidates, and the political system in general (Rid 2020: 400).

Chapter 2 State-sponsored disinformation

There are various terms used for disinformation such as misinformation and fake news. To understand disinformation, it is important to understand the intentions behind its usage instead of the method used for disseminating the information. Hence, the intention behind information dissemination determines the correct term.

This chapter serves as the theoretical framework of this research. First, the difference between various concepts in online misleading campaigns is explained. Secondly, the aim, the tactics, and the area of operations of disinformation campaigns will be explained. The overall aim of this chapter is to explain the concept of disinformation by answering the following sub-question: *What is disinformation, and how does it differ from propaganda used outside cyberspace?*

2.1 Disinformation, misinformation, and other concepts

Disinformation, misinformation, trolling, and fake news terms are closely related to each other. However, a distinction can be made based on the intent of the author. This paragraph aims to illustrate the difference between disinformation, misinformation, and trolling.

In this thesis, the term fake news will not be used. The main reason is that the term fake news is a contested one and has become contentious and politically motivated (Marwick & Lewis 2017: 44). Although the term fake news was first used to describe websites that intentionally posted clickbait, it is mostly known as a term adopted by the Trump's administration to discredit unflattering news items regardless of the news item is factually correct or incorrect and the intention of the author.

2.1.1 Disinformation

According to Fallis, disinformation has three characteristics. Firstly, disinformation is a type of information (Fallis 2015: 404). The second characteristic of disinformation is that it is not only information, it is a type of misleading information with the likelihood of creating false beliefs. These false beliefs could, potentially, have harmful consequences. The third and final characteristic of disinformation is the nonaccidental character. It must be no accident that the information is misleading. This last feature highlights the intent of the misleading information. Combining these three features will create the definition of disinformation.

Disinformation is misleading information that has the function of misleading (Fallis 2015: 401).

Disinformation has the function of misleading and therefore serves to benefit the source at the expense of the target (Lanoszka 2019: 229). However, disinformation is not a guaranteed success. Although it has the intention to mislead, the targeted audience can still not be misled by the information. This can be either a conscious or an unconscious decision. Furthermore, whether or not the targeted audience is misled, the actor is still distributing disinformation (Fallis 2015: 406). Hence, effectiveness does not play a role in classifying information as disinformation.

One of the persistent misconceptions of disinformation has to do with the factual correctness of the information. Disinformation is not simply fake or factually incorrect information. However, it could be (Rid 2020: 10). According to Wardle, disinformation can be divided into seven categories (2017):

1. Satire or parody;

2. False connection;
3. Misleading content;
4. False context;
5. Imposter content;
6. Manipulated content;
7. Fabricated content.

Wardle categorization places these seven types of disinformation on a scale, that loosely measures the degree of misleading intent of the author. Satire or parody has no intent to cause harm but has the potential to fool. A false connection is made when the headlines, visuals, or captions do not support the content of the message. Misleading content is the use of information to frame an issue or induvial in a certain way. Sharing genuine and authentic content with false contextual information is false context. Imposter content is the impersonation of genuine sources by the author. Manipulated content is the manipulation of genuine information or imagery with the intent to deceive. Lastly, fabricated content is the creation of a hundred percent false information designed to deceive and to do harm.

2.1.2 Misinformation and trolling

Misinformation and disinformation are often used interchangeably. The one-letter difference does not make it easier to make a clear distinction. However, there is a discrepancy between these two concepts. Misinformation is a more innocent form of misleading information since it does not have the intention to mislead. Misinformation can, for instance, be an honest mistake (Fallis 2015: 406). Hence, misinformation is *information that is incorrect by accident* (Lanoszka 2019: 229). Unlike disinformation, misinformation can never be a truthful statement.

2.1.3 Trolling

Trolling is another concept closely related to disinformation and misinformation. Trolling is an action performed by a troll. A troll is an actor who deliberately baits other people to elicit an emotional response (Marwick & Lewis 2017: 4). Although trolling is aimed to trigger a response by the target, it can also have more serious outcomes such as the destroying of someone's reputation or to reveal embarrassing information. According to Marwick & Lewis, trolls are apolitical and preferably use shocking imagery such as racist or sexist content as their tool for trolling (2020: 4). In today's digital era, trolling is an umbrella term that entails a wide variety of non-social internet behavior. The main goal of trolling is to provoke an emotional response. Trolls see trolling as a game and try to impress other trolls. Receiving an indignant, angry, or tearful response is the troll's ultimate goal. A successful troll plays with ambiguity in such a way that the targeted audience is never quite sure whether or not they are dealing with a troll (Marwick & Lewis 2017: 4-7).

2.2 Propaganda explained

According to Taylor, propaganda uses communication to convey a particular message, an idea, or an ideology that is primarily designed to serve the self-interest of the person or organization doing the communication. In essence, propaganda is no more than the communication of ideas designed to persuade people to think and even behave in a desired way. Hence, propaganda is about persuading people to do things that are beneficial to those doing the persuading. This can be done directly or indirectly. In addition, propaganda is not about wrong and right, it is about its intention which is to persuade people (2003: 6-7).

This research follows Taylor's definition of propaganda: *the deliberate attempt to persuade people to think and behave in a desired way* (2003: 6). In this definition, the means of communication does not determine whether or not it is propaganda. Just like disinformation, the intention of the initiator of the communication will determine the applicable label. Although this definition includes all types of propaganda, this research will predominately focus on the state's behavior.

The underlying assumption for propaganda is that information is power, and whoever controls the flow of information wields power over the recipient. According to Taylor, democratic societies exist based on consensus instead of coercion. Hence, persuasion is an integral part of the political process in democracies. Furthermore, persuasion plays a significant role in international relations related to the political, military, economic, and social instruments of power. Thus, in the power struggle, propaganda is an instrument used by those who want to secure or retain power (2003: 3-4).

2.2.1 Offline propaganda

Propaganda dates back to the time when humans began to communicate with each other, but the twentieth century has increased the scale on which propaganda has been practiced (Taylor 2003: 6). Thomas Rid has identified four waves of disinformation (2020: 6-7). Although Rid uses the term disinformation, this research will use the term propaganda to describe these four waves.

The first wave of modern-era propaganda identified by Thomas Rid started in the 1920s after the First World War and spans the Interbellum. Journalism was being reshaped by the rise of the radio. This created faster news coverage and a wider coverage area (Rid 2020: 6). The second wave of propaganda was formed after the Second World War. Propaganda became more professionalized and the Central Intelligence Agency (CIA) called this phenomenon political warfare (Rid 2020: 7). During the second wave, the goal was to *exacerbate existing tensions and contradictions within the adversary's body politic, by leveraging faces, fake, and ideally a disorienting mix of both* (Rid 2020: 7). The third wave started in the late 1970s and was a continuation of the second wave. According to Rid, propaganda became well-resourced, fine-tuned, and managed so the use of propaganda would be more effective (2020: 7). The third wave lasted until the start of the fourth and final wave mid-2010s. This last wave reshaped this domain through the use of new technologies and internet culture. It became an area of high-tempo, low-skilled, remote, and disjointed actions instead of the slow-moving, high-skilled, and labor-intensive campaigns it used to be (Rid 2020: 7).

2.2.2 Propaganda versus disinformation

Propaganda and disinformation are closely linked to each other. Disinformation is misleading information that has the function of misleading, and propaganda is the deliberate attempt to persuade people to think and behave in a desired way. Both concepts are nonaccidental types of information used in communication. Furthermore, by using disinformation and propaganda as an instrument, the initiator desires a certain outcome beneficial to itself. This can be anything between provoking certain reactions and international powerplay.

The main difference between disinformation and propaganda is the concept of misleading. This research argues that the different perspectives on the concept of misleading do not create a difference between disinformation and propaganda when it comes to the state's use of it. First of all, misleading is a matter of perception. One person's beliefs are another's lies (Taylor

2003: 6). So, what one person sees as misleading, another sees as truthful. Secondly, the use of propaganda to persuade others is in itself a form of misleading since the action has a desired outcome, to begin with. Here, the assumption is made that persuading the targeted audience is only necessary if the outcome would be different from what the initiator desired. Hence, propaganda and disinformation are the same concepts.

Although disinformation and propaganda are the same concepts, there might be a trend in the use of these concepts based on the level of digitalization of the activities. Offline activities are often described as propaganda. For instance, Taylor (2003) described the history of these activities starting in the Ancient World and ending around the year 2000 where he solely uses the term propaganda. Rid (2020) uses both propaganda and disinformation when describing offline campaigns. However, Rid does not use propaganda when it is related to online activities. This trend was observed in the various articles used for this research.

2.3 State-sponsored disinformation campaigns in practice

Disinformation can be a government effort aimed against foreign adversaries and their societies. If that is the case, Rid states that disinformation is not spontaneous lies of politicians, but it is the systematical output of large governmental institutes and has always been the playing field of foreign intelligence agencies (2020: 9).

The overarching term cyber troops will be used to describe governmental actors or state-sponsored actors that conduct disinformation campaigns. This term was introduced by Bradshaw & Howard (2017: 4) and refers to government or political party actors tasked with manipulating public opinion online. This definition reflects both important aspects of state-sponsored disinformation operators. Firstly, they operate in cyberspace, thus cyber. Secondly, troops imply an entity that has a combined effort to achieve a certain goal that has been set for or by them.

2.3.1 Targeting adversaries' societies

According to Rid, the method by which disinformation campaigns are executed is covert. However, their impact is often overt. Disinformation operators pretend to be something they are not. This tactic makes it harder for the targeted entity to detect the disinformation operator and the disinformation campaign.

The aim of the disinformation campaign can be anything and its intent is set by the entity conducting the campaign. As an example, the aim of a disinformation campaign can be executed with the intent to weaken the targeted advisory. In this example, disinformation can be used to create division between allied nations, to create tensions between ethnic groups within the adversary's territory, or to undermine the trust society has in (governmental) institutions (Rid 2020: 9). Disinformation campaigns can also have a more focused approach such as eroding the government's legitimacy or destroying the reputation of a certain individual (Rid 2020: 9).

Disinformation campaigns tend to erode the very foundation of open societies (Rid 2020: 11). In liberal societies, disinformation possess a threat since it could undermine their democratic institutions. However, this happens gradually and in a subtle manner. Once the authority of the evidence is eroded, emotions are there to fill in the gap. From that moment onward, making a distinction between facts and misleading facts becomes harder and harder

(Zelenkauskaite 2022: 134). This divide-and-conquer technique has the potential to create polarization within a society (Zelenkauskaite 2022: 81). However, a targeted society is not always helpless. The more robust a democratic society is, the more resistant it will be against disinformation campaigns. On contrary, weakened democracies succumb more easily to disinformation campaigns (Rid 2020: 10-11).

The ongoing digitalization of today's society changed the world of disinformation fundamentally. The internet made disinformation campaigns cheaper, faster, and less risky. Just like any type of digital information, false and misleading information can spread rapidly online (Schia & Gjesvek 2020: 414). The reason is that the internet and social media networks made it cheaper to do so (Nagasako 2020: 129). This is the result of the architecture of the internet and how information is shared and disseminated. One of the key characteristics of the internet is the irrelevancy of distance. The internet connects all users. Thus, all users all over the world can potentially interact with each other (Schia & Gjesvek 2020: 415).

These new forms of covert actions and new (online) forms of activism have made disinformation campaigns more scalable, harder to control, and harder to assess once they have been launched (Hunt 2021: 85). As a result, the internet has made open societies more open to disinformation (Rid 2020: 12-14, Schia & Gjesvek 2020: 414).

2.3.2 Strategies, techniques, and tools

Cyber troops can use a variety of strategies, techniques, and tools for their disinformation campaigns. As addressed before, these campaigns are not new. However, the presence of social networking technologies has changed the scale, scope, and precision of how disinformation campaigns are executed (Bradshaw et al. 2020: 11). First of all, the digitalized content can be disseminated on a large scale. As an example, posting certain content on Twitter will make that post potentially available to all Twitter users. Secondly, the internet connects all users. Therefore, cyber troops can direct their campaign to anyone. Anywhere. Lastly, the internet makes also it possible that people can connect to certain groups or individuals directly so cyber troops can focus their campaigns.

The strategy of cyber troops can be divided into four categories (Bradshaw et al. 2020: 15).

1. The creation of disinformation.
2. Profiling and targeting specific segments of the population with political advertisements.
3. The use of trolling, doxing[1], and online harassment.
4. Censoring speech and expression through the mass reporting of content or accounts.

The first type of communication strategy is the creation of misleading information such as misleading websites, doctored memes, altered images, and videos including deep-fake technologies. Bradshaw et al. argue that this is the most prominent type of communication strategy for cyber troops. The second category is the use of data-driven strategies to use advertisements to spread misleading information. The third strategy is the use of trolling, doxing, and online harassment. Although trolls are considered nonpolitical entities who bait other people to elicit an emotional response, cyber troops can use this strategy as well if it helps to achieve their misleading intent. In this scenario, the cyber troops use trolling and its outcome as a means to their political agenda. Lastly, cyber troops use the system against those

[1] Publishing personal information and documents about a person or organization (Schneier 2016).

with good intentions. They censor free speech and expression by mass-reporting of specific content or specific accounts. For instance, they report posts by journalists, activists, or political dissidents in a coordinated manner triggering the automated systems the social media companies use to flag, demote, or even take down inappropriate content. This last tactic will help their cause indirectly. By silencing the opponents, cyber troops could be in a more favorable position to disseminate and amplify their misleading message and content.

2.3.3 Where and how cyber troops operate

According to Marwick and Lewis, social and participatory media is key to the manipulation of the mainstream media (2017: 24). Blogs, forums, and message boards are important information hubs where people can find like-minded others and disseminate knowledge. Many of these websites facilitate interaction extensively. Users can link to each other, engage with each other's content, and quote each other making it an ideal location to post and amplify misleading information. Mainstream social media platforms such as Twitter, Facebook, and Instagram are perfect locations to post and amplify misleading information (Marwick & Lewis 2017: 26). Private groups can echo messages via these networks (Marwick & Lewis 2017: 18).

Cyber troops operate covertly and preferably on a large scale. To do so, they use both real and fake accounts to spread their misleading information. These accounts can be operated by humans, but they can also be automated making them even more scalable (Bradshaw et al. 2020: 11). Especially these automated accounts can be used to amplify certain narratives on a large scale (Bradshaw et al. 2020: 11). Amplification of one's message will lead to the demoting of other's content.

A distinction can be made between human-operated accounts and automated ones according to Bradshaw et al. (2020: 11). Both types of accounts have their advantages. Human-operated accounts are not as scalable as automated ones, but they can be used in a more precise manner. Human-operated accounts can engage in conversations by posting comments or tweets, or by private messaging individuals via social media platforms. Bradshaw et al. have identified human-operated accounts that were hacked, stolen, and even impersonated. However, these types of accounts are only a small portion of account types involved in disinformation campaigns (2020: 11). Automated accounts are also known as bots and they increase the spread and reach of misleading content significantly since the more popular content is, the more it will be shown to other users. (Rogers & Niederer 2019: 8).

Bradshaw et al. have identified three types of messaging techniques cyber troops can when they are operating online (2020: 13). The first is to artificially amplify content that favors their desired outcome. The second technique is to amplify negative content regarding the targeted population. For instance, cyber troops amplify the positive messages about person A but also amplify the negative messages about person B. The third technique is to silence others via trolling, doxing, and online harassment so others cannot oppose the misleading content.

2.4 Conclusion

Disinformation is the unaccidental spread of misleading information for the purpose of misleading. This is contrary to the term misinformation which is the spreading of incorrect content by accident.

Cyber troops conduct disinformation campaigns to purposefully mislead targeted advisories. To remain covert, they hide amongst other online users and even imitate other tactics such as trolling. However, state-sponsored disinformation is always a politically motivated campaign aimed to enforce a certain outcome.

Chapter 3 The evolution of disinformation and securing cyberspace

The insider threat

Disinformation is not a new phenomenon (Taylor 2003: 6, Rid 2020: 6-7). Disinformation is closely related to propaganda and is being used as a synonym. Since propaganda existed since ancient times (Taylor 2003: 6), disinformation is also as old as mankind. Yet, these concepts did not found their way into cyberspace (yet).

However, with the ever-evolving digitalization of modern society, it was inevitable that propaganda would become part of cyberspace. Especially since cyberspace was becoming more important in international politics and was gaining more attention. This chapter aims to answer the following question: *How is disinformation deployed in this phase, how is it perceived, and which attempts are made to mitigate the impact of disinformation?*

3.1 Propaganda meets the online world

Traditionally. propaganda has been disseminated by word of mouth or printed pamphlets which were distributed through a known network (Crilley 2001: 250). According to Crilley, the rise of the internet has made information widely available and created wider coverage with a more diverse audience than ever before. In addition, the use of the internet has several advantages over traditional methods of publishing. First of all, the use of the internet for the dissemination of content can bypass national laws (Crilley 2001: 251). Secondly, it is more cost-efficient and therefore, lowers the threshold for participating (Whine 1999: 236).

The advantages of the internet for propaganda purposes were noticed by various groups and organizations. According to Theohary and Rollins, the internet was used by international insurgents, jihadists, and terrorist organizations as a radicalization and recruitment tool, a communication method, and a method of the distribution of propaganda (2011: 2-4). They used chat rooms, dedicated servers and websites, and social networks as a platform for the dissemination of their content. The internet was the terrorists' prime recruiting tool and it was being used for fund-raising activities via cybercrime activities (Theohary & Rollins 2011: 2). The way the internet is built, helps to facilitate communications of decentralized entities. For instance, Al Qaida has transformed itself into a diffuse global network composed of dispersed nodes with varying degrees of independence (Rollins 2011). Therefore, the decentralized way the internet is designed and the associated difficulty in responding to emerging threats matched the franchised nature of terrorist organizations and their operations (Theohary & Rollins 2011: 2).

As described above, terrorists and their organizations used the internet for various purposes. However, the Federal Bureau of Investigation (FBI) did not assess that terrorists were capable of performing cyber-attacks (Chabinsky 2009). Former FBI Director Robert Mueller stated during his testimony regarding the 2007 Annual Threat Assessment, that *terrorists increasingly use the Internet to communicate, conduct operational planning, proselytize, recruit, train, and to obtain logistical and financial support. That is a growing and increasing concern for us*" (Theohary & Rollins 2011: 5). It seems to be that the focus of the FBI was on online activities of terrorist organizations by monitoring these activities. Although terrorist organizations were not (yet) capable of performing a terrorist cyber-attack, the Congressional Research Service portrays

the potential objectives of such an attack (Theohary & Rollins 2011: 5). These four objectives are:

1. The loss of integrity of information in such manner that the information be modified improperly;
2. The loss of availability of mission-critical information systems;
3. The loss of confidentiality of information to unauthorized users;
4. The physical destruction of property via the creation of actual physical harm through commands that cause deliberate malfunctions.

While the FBI scoped its operations to monitor the online activities of these malicious groups, another US governmental organization added another dimension to their activities. The National Security Agency (NSA) also took down malicious websites (Nakashima 2010).

Not only terrorist organizations used the internet to their advantage. American Far Right groups, US militant movements, and German neo-Nazi groups used the internet for propaganda purposes (Whine 1999: 235-236). All of these groups have in common that they are non-state groups and organizations that operate in a decentralized manner. However, it appeared that in the early days of the internet, states did not use the internet for propaganda purposes at that time.

3.2 US's perspective on keeping cyberspace safe

It appeared to be that online information itself was not in full scope by the US government. Online information of non-state hostile groups and organizations was mostly monitored, and occasionally taken down to keep society safe. It seems like these non-state actors used the advantages of the internet and the digitalization of modern society for their propaganda activities in the same way they would have done it in an offline setting. The internet made it only easier, cheaper, and more effective. This has been noticed by the FBI and other federal government organizations and their focus was primarily on monitoring the online activities of these malicious non-state actors (Rollin & Theohary 2011: 6-8). However, the NSA has demonstrated that they also took down malicious websites (Nakashima 2010).

At that time, the focus on keeping cyberspace safe was built on three concepts: Confidentiality; Integrity; and Availability. These are also known as the CIA-triad (Samonas & Coss 2014: 26-29). At the same time the FBI was focused on the online activities of various malicious non-state groups and organizations, the United States faced two major leaks of confidential governmental information. In 2010 the twenty-two-year-old Army private Bradley[2] Manning leaked more than seven hundred thousand classified documents from the US State Department and the Department of Defense. Three years later, Edward Snowden stole and leaked classified information from the NSA (Rid 2020: 339-340).

3.3 Lessons learned and policies for the future

The major impact of the unwanted leaking of classified information can be seen in various policy documents from this particular timeframe (2008-2015). The most important documents for the US federal government operating in cyberspace are the National Security Strategy

[2] At the time of the leak private Manning first name was Bradley. This was later changed into Chelsea.

(NSS) and the National Defense Strategy (NDS). The focus of the analysis of these strategic documents is on cyberspace and the threats in cyberspace.

3.3.1 The National Defense Strategy 2008

The 2008 version was the successor of the 2005 version. The NDS 2008 was built upon the lessons learned from previous operations and strategic reviews. Furthermore, the NDS 2008 was built upon the foundation of the NSS 2006. The main pillars of the NSS 2008 were *promoting freedom, justice, and human dignity by working to end tyranny, promote effective democracies, extend prosperity; and confront the challenges of our time by leading a growing community of democracies. It seeks to foster a world of well-governed states that can meet the needs of their citizens and conduct themselves responsibly in the international system. This approach represents the best way to provide enduring security for the American people* (US Department of Defense 2008: 1).

In conclusion, the strategic path of the United States since 2008 was to see the use of malicious activities in cyberspace in relation to the disruption of the US society or as an enabler for military effects on the (future) battlefield. The NDS 2008 links cyberspace to the protection of systems and processes and these two aspects are the core of integrity and availability of the CIA-triad. It is worth mentioning that the strategic focus of the NDS 2008 is not information and disinformation but solely on the protection of critical infrastructure from disruption and sabotage.

3.3.2 National Security Strategy 2015

In February 2015 the White House published a new NSS. The world became more and more digitized which is also reflected in this version of the NSS. Two aspects can be identified based on the strategic intentions within cyberspace in the NSS 2015. These aspects are the protection of critical infrastructure against cyberattacks and the protection of information vital to the government of the United States or its economy. These were similar to the strategic goals of the NDS 2008.

Thus. the focus on cyberspace was still directed toward the protection of critical infrastructure from disruption and sabotage. Information itself was not seen as a focus of cyberspace. This omission indicates that the US was not expecting a national security threat against information itself.

3.4 Conclusion

Cyberspace has become an emerging area within international politics. However, the propaganda of nation-states has not made its way into the digital world (yet). Only non-state groups and organizations were conducting online propaganda activities. Although this was of concern to the United States, it was not a concern in keeping cyberspace safe from adversarial states.

The protection of cyberspace has traditionally focused on securing information, maintaining the integrity of information, and keeping systems and digitalized processes available. Major events for the United States were the leaking of classified government documents and the leaking of NSA's espionage tools and tradecraft.

The strategic documents of the US government set the direction for the near future. Cybersecurity should protect the confidentiality of the information and keep critical processes and systems operational. In this period, there was no focus on the information itself.

Chapter 4 The 2016 US Presidential Election and its aftermath

The tipping point

The rise of social media fitted the US' belief in a free flow of information in an open democratic society. At the same time, cyberspace became more and more contested. Malicious entities found their way to the online realm. Yet, they were non-state actors and entities that used the internet for their online propaganda activities. The appropriate response from the US federal government was primarily to monitor these activities (Rollin & Theohary 2011: 6-8).

While these monitoring activities continued, another online threat would manifest itself during this particular period in time. This period is marked by the upcoming Presidential Election on November 16, 2016, and can be seen as the tipping point in the transformation of disinformation in cyberspace. It was the first time that a state conducted an online disinformation campaign aimed against another state which was not part of a hybrid war (Splidsboel Hansen 2017: 4). In this case, Russia conducted a disinformation campaign against the United States (Rid 2020: 400).

During the Cold War, the Soviet Secret Service *Komitet Gosudarstvennoi Bezopasnosti* (KGB) practiced active measures against the United States. The end of the Cold War and the collapse of the Cold War did not end these types of operations (Hosaka 2020). A digital forensic investigation of the hack on the Democratic National Convention showed that both KGB's successors, the GRU and the SVR, continued Russian influence operations against the United States.

This chapter aims to answer the following sub-question: *How is disinformation deployed in this phase, how is it perceived, and which attempts are made to mitigate the impact of disinformation?*

4.1 Significant offensive actions in cyberspace

Online malicious actions against the United States during the 2016 US Presidential Election can be divided into two events. The first event is the hack of the Democratic National Convention (DNC) and the stealing of confidential information from the DNC. This event was executed by Russia since it was attributed to Russian military intelligence and Russian foreign intelligence services (Alperovitch 2016). The other event is the leaking of these stolen confidential documents. The latter event was been visible during the election and details came to light after the election.

4.1.1 The hacks on the democratic party

In march 2016, the Russian military intelligence service (GRU) started its offensive campaign against the potential democratic presidential candidate Hillary Clinton and their first attempt was a phishing campaign directed toward Clinton's campaign headquarters (Jun 2016: 354, Rid 2020: 379). This attempt failed since their email security required multifactor authentication. Therefore, the stolen credentials were not enough for the GRU to gain access to the targeted systems (Rid 2020: 379). After this unsuccessful attempt, the GRU aimed their efforts at the private email accounts of members of the Clinton campaign (Johns & Riles 2016: 350, Rid 2020: 379, Volkov 2019: 60). Since these private email accounts were less protected, the GRU was successful and gained access to the account of the chairman of the Clinton campaign (Rid 2020: 379). This access allowed the GRU to exfiltrate over fifty thousand emails from the chairman's compromised email account (Rid 2020: 380). The GRU continued its

successful cyber campaign and eventually gained access to the Democratic Congressional Campaign Committee (DCCC), the organization supporting the Democrats in the House of Representatives (Alperovitch: 2016, Rid 2020: 382).

The GRU's access to the systems of the DCCC enabled them to intercept additional login and password credentials. These credentials were linked to the systems of the Democratic National Convention (DNC) and allowed the GRU to pivot from the systems of the DCCC towards the systems of the DNC. Once inside the systems of the DNC, the GRU searched for files related to the highly contested presidential campaign (Rid 2020: 383). In the meantime, the GRU purchased a domain called *DCLeaks.com* which they were planning to use as a platform for leaking stolen documents. However, no documents related to the presidential campaign and election were published on the website (Rid 2020: 383).

On April 28, 2016, the IT staff at the DNC detected unauthorized users on their network. The DNC hired cybersecurity firm CrowdStrike to investigate the unauthorized access and to clean up the systems of the DNC. CrowdStrike found digital evidence of not one but two sophisticated adversaries on the systems of the DNC. Not only the Russian military intelligence service gained access, but the Russian foreign intelligence service (SVR) also had access to the systems of the DNC. Interestingly, CrowdStrike did not find any evidence of collaboration between the GRU and the SVR inside the systems of the DNC. CrowdStrike assumption is that neither organizations were aware of the presence of the other (Rid 2020: 383-385).

On June 14, 2016, the double hack on the DNC was made public (Rid 2020: 386). The Washington Post revealed that foreign spies gained access to the entire database of the DNC. This database contained opposition research on the Republican presidential candidate Donald Trump. CrowdStrike released a technical report regarding the hack on the DNC and exposed the Russian digital tradecraft. The GRU and SVR had to take down their offensive infrastructure and rebuild it before they could execute other offensive cyber operations (Rid 2020: 386).

4.1.2 Guccifer 2.0

The revelation of the Russian hack on the DNC did not stop the GRU. Their next step was the creation of the persona Guccifer 2.0. During the tumult of the hack on the DNC, a Romanian hacker called Guccifer claimed that he hacked Hillary Clinton's mail server. The GRU build upon this legend and created a blog at *https://guccifer2.worldpress.com*. On June 15, 2016, a post from Guccifer 2.0 went online. This post dismissed CrowdStrike's conclusion and stated that the DNC had been *hacked by a lone hacker* (Rid 2020: 387-388). Eleven documents were published on the blog site. Amongst these documents was an opposition research file on Donald Trump.

However, these eleven files were not taken from the DNC as Guccifer 2.0 claimed. These files were stolen from the DCCC's chairman's email account. The GRU not only made a false claim of the origin of the documents but the documents were also tampered with. This was revealed via the hidden metadata. Five files were modified just before the publication and four of them were labeled as confidential or even secret. Several technical journalistic investigators discovered additional metadata to the files and tied these fabricated files to the Russian GRU. Interestingly, the US intelligence community did not confirm the claims made by the

Democrats, CrowdStrike, and other correspondence regarding the hack and leak on the DNC (Rid 2020: 388-392).

Guccifer 2.0 also operated on the social media network Twitter and allowed anyone to contact this online persona of the GRU. Julian Assange used Twitter to talk to Guccifer tor to use WikiLeaks as a platform for leaking stolen documents. WikiLeaks published almost twenty thousand emails including more than eight thousand attachments three days before Democratic National Convention. During this convention, the Democratic Party would announce its presidential nominee. The GRU used several means of dissemination. First of all, they used WikiLeaks and their blog site for publishing documents. Secondly, they used front accounts such as *@DCLeaks* to correspond with various news and media outlets in the United States and internationally. At that point in time, leaks were considered a legitimate source of news. It was still assumed that the accounts leaking information were distributing original and unmodified documents (Rid 2020: 392-394).

On October 7, 2016, the US Intelligence community called out the Russian digital campaign. They stated that Guccifer 2.0 and *@DCLeaks* were Russian intelligence fronts. WikiLeaks used this tumult to publish the entire inbox of the DCCC's chairman. This was not a single dump, WikiLeaks published a batch every day until the 2016 Presidential Election. Although the intelligence fronts were exposed, the GRU still used these means to reach out to journalists. In the end, the front accounts interacted with over twelve hundred users and exchanged around fifteen thousand direct messages (Rid 2020: 395).

4.2 Targeted advertisements

The 2016 Presidential Election was also theater to a new way of digital influence. A British consulting firm called Cambridge Analytica was able to combine psychological profiling and powerful machine learning in the political debate and electoral process (Hankey et al. 2018). Whether or not Cambridge Analytica obtained the information via the user's consent is irrelevant to this research and will not be further addressed. An app called *thisisyourdigitallife* collected the data of over three hundred thousand Facebook users and their Facebook friends (Schneble et al. 2018). Cambridge Analytica used this data to create individual profiles of over two hundred million US citizens. Cambridge Analytica's services were used to create targeted advertisements for political campaigns including Donald Trump's Presidential campaign (Hankey et al. 2018).

Cambridge Analytica claimed to have between five thousand and seven thousand data point on over two hundred million citizens in the United States. These data points were then paired against the OCEAN[3] personality score. This would create a psychographic political profile of the individuals in their database. These profiles were then connected to the existing dataset of

[3] *The OCEAN (or 'Big Five') personality system identifies five independent personality traits. The original research was published in 1990. Unlike many models of personality, which are driven by an expert's theory about how humans differ from one another, the Big Five model was created by data-driven statistical methods. The underlying assumption is that if a trait is important in distinguishing humans from one another, then there will be many adjectives in the dictionary that make that distinction. For example, we might call someone talkative, sociable, outgoing, excitable, friendly, gregarious, or unreserved, and all of these words have an underlying commonality which is extroversion. The Big Five traits are Openness, Conscientiousness, Extraversion, Agreeableness and Neuroticism. All humans can be compared across the five traits, and personality tests measure where an individual scores on each of the personality traits* (Hankey et al. 2018: 17).

the Trump campaign. As a result, the Trump campaign was able to target voters on an individual level instead of on a group level. This was done via the creation of tailored messaging and content. Furthermore, the data also allowed the identification of voter blocks in the crucial key battleground states (Hankey et al. 2018).

4.3 Lessons learned and policies for the future

The United States faced two new forms of influence campaigns during their 2016 Presidential Election. Hacking and leaking information were not new a phenomenon, as seen by the actions of Manning and Snowden. However, Russia added another dimension to the hacking and leaking of confidential information. They also manipulated these documents before leaking them and this was something not observed before. This new tactic did not only affect the confidentiality of information, but it also affected the authenticity of the information, thus the quality of information. The second new form was the use of personal data for a data-driven political campaign by Cambridge Analytica which was proven to be a very effective tool during the Presidential campaign (Hankey et al. 2018).

Both created a public debate and gained worldwide media attention. One of the concerns was about social media. Social media platforms, like Twitter and Facebook, have a different structure than traditional media. Content can be disseminated easily between users without any third-party filtering, fact-checking, or editorial judgment. Individual users can, even with no track record or reputation, reach as many readers as Fox News can reach (Alcot & Gentzkow 2017: 211).

It remains unclear if this public attention was fueled by the winning of Donald Trump since this outcome was unexpected to some people (Bateson & Weintraub 2022: 2301). Alcot and Gentzkow argue that the influence of disinformation was not pivotal for the election since the percentage of voters that were influenced is much smaller than Trump's winning margin in the crucial states (2017: 232). Grinberg et al. also claim that Russia-sponsored content on social media likely did not decide the election (2019: 377). On contrary, Jamieson stated that a combination of Russian trolls and hacking likely tipped the election favorably for Donald Trump (2018). The different opinions on the influence of the Russian disinformation campaign illustrate that it is impossible to determine a possible outcome of an event that did not take place or to change some variables of an event and determine a hypothetical outcome based on these variables. Therefore, it is possible that the Russian disinformation campaign may have influenced the outcome of the US 2016 Presidential Election.

The US Senate Intelligence Committee commissioned two studies to investigate the disinformation campaigns targeting hundreds of millions of US citizens during the 2016 Presidential Election (Aral & Eckles 2019: 858). However, it would take months, and even years of congressional hearings and investigations to fully see the magnitude of both types of influence campaigns.

4.3.1 The accessibility of manipulated content

A tipping point in this influence operation is the use of manipulated and fabricated content by Russia as part of its disinformation campaign. This was different from the previous experience of hacking and leaking confidential documents and information. This tactic created a new dimension to the threats in cyberspace. Up until the 2016 election, information was to

be protected. Now Russia has demonstrated that the quality and authenticity of information were also contested.

Congressional hearings and an investigation by the US Federal Trade Commission (FTC) on the role of social media platforms and the distribution of manipulated media showed the magnitude of Russian online activities. Politico published a story in October 2017 that Facebook has identified eighty thousand Russia-linked posts on its platform that sought to interfere in the 2016 US Presidential Election and that these posts were viewed by over one hundred twenty million users (Scola & Gold 2017). With hindsight, these posts were planted on Facebook by the Russian Internet Research Agency (IRA) between January 2015 and August 2017. In addition, Facebook announced to congressional investigators that three thousand online political advertisements were linked to the same IRA. These advertisements were seen by more than eleven million people (Scola & Gold 2017).

Twitter stated that over thirty-six thousand automated accounts were possibly linked to Russia and that these accounts generated almost one-and-a-half million election-related tweets during the 2016 US Presidential Election. These tweets were viewed about 288 million times (Scola & Gold 2017). Additionally, almost three thousand Twitter accounts were linked to the IRA.

These numbers of manipulated and fabricated content and the way algorithms of social media work is a dangerous combination. What a user sees on their Facebook timeline is not a derivative of a person's interests. It is a reflection of what Facebook determines you will be interested in. This will create an information bubble where shown content is based on your online activity (Hankey et al. 2018).

4.3.2 Political advertisements

The algorithms for the creation of information bubbles on social media were also used to target specific users for political ends. To complicate matters, the architecture of social media platforms made it difficult to trace advertisements for political use since it did not treat political advertisements differently than commercial ones. Furthermore, the adverts do not stay with the user. Advertisements disappear so they were never examined and have therefore not led to any debate (Hankey et al. 2018).

It remains unclear if Donald Trump would have won the 2016 Presidential Election without the services provided by Cambridge Analytica. However, Donald Trump winning this election and becoming the president of the United States has led to controversy. The revelations about Cambridge Analytica have demonstrated the extent to which data-driven microtargeting can be used for manipulation in democratic elections in the United States and possibly in the rest of the world (Hankey et al 2018).

4.4 Conclusion

In this period, the United States saw cybersecurity as keeping cyberspace safe via the protection of the confidentiality of the information and keeping critical processes and systems operational. The start of the 2016 Presidential Election started with the Russian hacks on the Democratic presidential campaign. These actions were in line with the strategic directions shaped by the White House and the Department of Defense. However, all shifted subtly since the GRU not only leaked stolen documents and information but also altered and manipulated

this content. This created a situation that the United States did not anticipate forehand, securing cyberspace is not only about the confidentiality, integrity, and availability of information. It is also about the quality of the content and its originality. This new threat was further amplified by the manipulative way political advertisements were being used and distributed amongst social media platforms.

So, on-hand information shown online, and even via legitimate news outlets, could be manipulated or even fully fabricated. On the other hand, political advertisements were tailored-made psychological constructs to influence voter behavior. The 2016 Presidential Election has shown the vulnerability of an open democratic society regarding (foreign) influence operations. Online disinformation campaigns from one state to another saw the light during the 2016 US Presidential Election.

Chapter 5 The 2018 US Midterm Elections

The limited toolbox

The 2016 US Presidential Elections demonstrated the vulnerabilities of a free and open society. The way Russia executed its interference campaign during the US 2016 Presidential Election came as a surprise and has created political attention for state-sponsored disinformation campaigns. It drove the question of how to best combat these foreign campaigns in a society known for the free flow of information. Furthermore, the US underestimated the influence social media companies have regarding content on users' timeline due to the structure of social media. Users generally read information that is ideologically quite similar to their own beliefs and users that regularly read partisan articles are almost exclusively exposed to only one side of the political spectrum. Therefore users are likely to consume only content that aligns with their own beliefs. This phenomenon is known as echo chambers (Flaxman et al. 2016: 299). These echo chambers lead to information bubbles where users are largely exposed to information confirming their opinions.

Russia's disinformation campaign during the 2016 US Presidential Election sowed division in the society of the United States. Although it looks like it is impossible to prove the extent to which Russia's actions influenced this election, it is presumable that it put the US society's belief in fair and honest elections to the test. Disinformation was not something that could be easily spotted and countered. If the United States wanted to prevent Russian, and other foreign, interference campaigns during the US Midterm Election of November 6, 2018, they needed to change their strategy, posture, and cyber capabilities. This chapter aims to answer the following question: *How is disinformation deployed in this phase, how is it perceived, and which attempts are made to mitigate the impact of disinformation?*

5.1 The Internet Research Agency

The Internet Research Agency (IRA) operated from St. Petersburg in Russia. Besides the IRA, they are also known as the Troll Farm. Although this name has an innocent touch, they can be labeled as cyber troops since they are manipulating public opinion online for a political goal.

The initial focus of the IRA was in favor of Russian activities in Crimea, Ukraine. Already in 2014 and two years before the contested 2016 US Presidential Election, the IRA expanded its focus and activities toward the United States. According to Thomas Rid, the assignment of the IRA's American Department was to *spread distrust toward the candidates, and the political system in general* (2020: 400).

The IRA was evolving and they became more skilled and more knowledgeable about things such as operational security. They procured computer infrastructure and servers within the United States and they acquired server space on US-based servers so they could set up a secure and obscure connection between St. Petersburg and the United States via Virtual Private Networks (Rid 2020: 403). This allowed the operators of the IRA to use encrypted tunnels while routing their disinformation toward the US. This tactic made it hard for social media, and other Big Tech companies to discover Russian disinformation campaigns on their platforms.

5.2 Strategies and policies

In December 2017, the White House released its National Security Strategy. A month later the US Department of Defense released its National Defense Strategy 2018 which was called *Sharpening the American Military's Competitive Edge*. Before the 2016 Us Presidential Election, the quality of information was not in the US government's scope. The Russian disinformation campaign of 2016 could have influenced the outcome of the Presidential Election and the US government became aware of this possibility. This is reflected in the strategies and policies of this period because both the NSS 2017 and the NDS 2018 took information warfare and disinformation into account. In the previous versions of these strategies, the US government did not mention those concepts. This indicates that the United States was expanding its focus on keeping cyberspace safe by also focusing on information itself.

5.2.1 National Security Strategy 2017

Cyberspace was at the forefront of the NSS 2017. The focus in cyberspace was no longer solely on the protection of critical infrastructure against cyberattacks and the protection of information vital to the government of the United States or its economy. The White House's first pillar of four is the protection of the American people, their homeland, and the American way of life. Under this pillar, there is the strategic intention to *Keep America Safe in the Cyber Era*. Furthermore, the NSS 2017 states that *America's response to the challenges and opportunities of the cyber era will determine our future prosperity and security* (The White House 2017: 12). This notion implies that both their reactions to adversarial actors and their actions will be of vital importance for the future of United States. Just like the NSS 2015, the 2017 version still saw cyberattacks something that could damage or disrupt critical infrastructure in the United States.

The White House has identified five priority actions within the cyber domain (2017: 13):

1. Identify and prioritize risk;
2. Build defensible government networks;
3. Deter and disrupt malicious cyber actors;
4. Improve information sharing and sensing;
5. Deploy layered defense.

The five priorities within the cyber domain illustrate the strategic intention of the United States for the upcoming years. Their aim in cyberspace was to improve the security and resilience of their critical infrastructure based on six domains: *national security, energy and power, banking and finance, health and safety, communications, and transportation*. The defense of these domains will be prioritized on the assessed consequences and effects. Secondly, the US government will upgrade its digital defense so it can provide uninterrupted and secure communications and services under all conditions. To prevent attacks, the federal government will ensure that the necessary information is shared amongst government and non-government entities. The US will work with the private sector to remediate known malicious activity at the network level. On an international level, the US will work with its allies to expand awareness of malicious activities. And lastly, the *United States will impose swift and costly consequences on foreign governments, criminals, and other actors who undertake significant malicious cyber activities.*

A new concept mentioned in the NSS 2017 is disinformation which is mentioned under the third pillar *Preserve Peace Through Strength*. In this section, the White House states: *Malicious state and non-state actors use cyberattacks for extortion, information warfare, disinformation, and more. Such attacks can harm large numbers of people and institutions with comparatively minimal investment and a troubling degree of deniability. These attacks can undermine faith and confidence in democratic institutions and the global economic system* (2017: 31). One of the US' priorities in cyberspace is to improve attribution, accountability, and response to malicious activities. This indicates that the United States not only wants to attribute cyberattacks and other malicious behavior in cyberspace, but they also want to respond to this behavior. This will be achieved by enhancing their cyber tools and capabilities and improving their agility. The White House sees an important role for the US Intelligence Community in *this information-dominant era* (The White House 2017: 32).

Information is being weaponized by the adversaries of the United States. Their adversaries use this weaponized information *to attack the values and institutions that underpin free societies while shielding themselves from outside information. They exploit marketing techniques to target individuals based on their activities, interests, opinions, and values. They disseminate misinformation and propaganda* (NSS 2017: 34). The Whites House's concern is that their advisories integrate publicly available data with the data their intelligence agencies intercepted and collected, and use machine learning and Artificial Intelligence capabilities for further data analytic capabilities. Russia is mentioned specifically concerning information operations. The White House sees Russia using these types of operations as part of its offensive cyber campaigns to influence public opinion across the globe. This was made clear during the 2016 US Presidential Election. to mitigate such information operations, the US *will craft and direct coherent communications campaigns to advance American influence and counter challenges from the ideological threats that emanate […] competitor nations. These campaigns will adhere to American values and expose adversary propaganda and disinformation* (The White House 2017: 35).

5.2.2 National Defense Strategy 2018

The first thing noteworthy of the NDS 2018 is that the United States acknowledges that cyberspace is contested. The Department of Defense identified the United States as a target for malicious cyber activity against personal, commercial, government infrastructure, and political and information subversion (US Department of Defense 2018: 3). Although is not labeled as such, this notion is in line with the White House's strategy for influence operations.

Sea, air, and land are the classical military domains. Cyberspace is in the NDS 2018 labeled as a warfighting domain. Therefore, the Department of Defense will *invest in cyber defense, resilience, and the continued integration of cyber capabilities into the full spectrum of military operations* (US Department of Defense 2018: 6). These investments will *also prioritize capabilities to gain and exploit information, deny competitors those same advantages, and enable us to provide attribution while defending against and holding accountable state or non-state actors during cyberattacks*.

The overall outline of the NDS 2018 is predominantly on classical warfare. However, the US attitude is not passive anymore. In line with the NSS 2017, the Department of Defense will prepare itself for a digital engagement with its adversaries. In addition, they have the intention not only to engage but also to attribute malicious activities in this domain. Lastly, the US Department of Defense states that the NDS 2018 underpins their planned fiscal year 2019-2023 budgets meaning their strategic intentions will also be operationalized (US

Department of Defense 2018: 6). It seems to be that the United States had established a different mindset when it comes to cyberspace and the malicious activities within.

5.3 The indictment

The investigation of the Russian disinformation campaign was in full swing during this period. On May 17, 2017, the US Department of Justice (DOJ) appointed former FBI director, Robert Mueller as a Special Counsel for the FBI investigation of Russian government efforts to influence the 2016 Presidential Election and related matters (Rosenstein 2017).

In February 2018, the DOJ announced the indictment of thirteen Russian nationals for meddling in the 2016 US Presidential Elections (Mueller 2018). According to the thirty-seven-page-long indictment, the IRA *had a strategic goal to sow discord in the U.S. political system, including the 2016 U.S. presidential election. Defendants posted derogatory information about a number of candidates, and by early to mid-2016, Defendants' operations included supporting the presidential campaign of then-candidate Donald J. Trump ("Trump Campaign") and disparaging Hillary Clinton. Defendants made various expenditures to carry out those activities, including buying political advertisements on social media in the names of U.S. persons and entities. Defendants also staged political rallies inside the United States, and while posing as U.S. grassroots entities and U.S. persons, and without revealing their Russian identities and [IRA] affiliation, solicited and compensated real U.S. persons to promote or disparage candidates. Some Defendants, posing as U.S. persons and without revealing their Russian association, communicated with unwitting individuals associated with the Trump Campaign and with other political activists to seek to coordinate political activities* (Mueller 2018: 4).

The FBI investigation and the indictment gave more insight into the actions of the IRA. Around the summer of 2016, the IRA began to promote allegations of voter fraud executed by the Democratic Party. They used fictitious US personas and their front groups on social media for these claims. In addition, they also used advertisements during their disinformation operations. These purchased advertisements on Facebook were used to further promote these conspiracies (Mueller 2018: 18-19). The IRA continued the use of advertisements and expanded their way of working by also producing advertisements. These advertisements were advocating in favor of Donald Trump and were opposing Hillary Clinton (Mueller 2018: 19). The indictment demonstrates the direct link between the targeted advertisements and the Russian disinformation campaign.

The indictment drew a line where the United States took a stand on what was tolerated and what was not. The US did not tolerate foreign disinformation operations against the US and its political system in general. However, the US did not challenge disinformation at the level of the information itself. They engaged in disinformation more in an abstract manner. This might be of added value for international relations, but it did not contest the actual misleading information. The misleading information was not exposed and as a result, it was unclear which information was part of Russia's disinformation operations and which information was not. This left room for debate.

5.4 The political response of the United States

In this period, it was uncertain how the US would respond if the IRA would continue its disinformation operations since it was foreseeable that President Trump saw the IRA and Russia as an ally that helped him in the race for the White House.

On September 12, 2018, President Trump issued an Executive Order *Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election* (Trump 2018). The Executive Order states *that the ability of persons located, in whole or in substantial part, outside the United States to interfere in or undermine public confidence in United States elections, including through the unauthorized accessing of election and campaign infrastructure or the covert distribution of propaganda and disinformation, constitutes an unusual and extraordinary threat to the national security and foreign policy of the United States*. The Executive Order demonstrates that the US does not tolerate foreign interference in their democratic process.

This Executive Order was followed by a Joint Statement released via the Office of the Director of National Intelligence (ODNI) on October 19, 2018 (Director of National Intelligence 2018). This press release expresses the concern of foreign influence campaigns *undermine confidence in democratic institutions and influence public sentiment and government policies. These activities also may seek to influence voter perceptions and decision-making in the 2018 and 2020 U.S. elections.* The ODNI has identified various forms in which foreign actors execute their influence campaigns such as the use of social media to amplify divisive issues, sponsoring specific content, seeding disinformation regarding political candidates via sympathetic spokespersons, and dissemination of foreign propaganda. Foreign powers have exploited America's free and open political system, but that will not be tolerated anymore.

A second Joint Statement was released one day before the 2018 Midterm Elections on November 5, 2018 (Department of Homeland Security 2018). In their press release, the Department of Homeland Security (DHS), the DOJ, the ODNI, and the FBI stated that they *have been working in unprecedented ways to combat influence efforts and to support state and local officials in securing our elections, including efforts to harden election infrastructure against interference. Our goal is clear: ensure every vote is counted and counted correctly. [...] But Americans should be aware that foreign actors – and Russia in particular – continue to try to influence public sentiment and voter perceptions through actions intended to sow discord. They can do this by spreading false information about political processes and candidates, lying about their interference activities, disseminating propaganda on social media, and through other tactics. The American public can mitigate these efforts by remaining informed, reporting suspicious activity, and being vigilant consumers of information, as discussed below.*

The United States government will not tolerate foreign interference in their elections and the US will not hesitate to defend its electoral process or punish those who interfere in it.

5.5 The operational response of the United States

In the background, the Pentagon has empowered US CYBERCOM to build a far more aggressive approach in its mission to defend the US against cyberattacks (Sanger 2018). Up until then, US CYBERCOM had a more defensive posture helping to counter cyberattacks. Their new objective is to *contest dangerous adversary activity before it impairs [the United States]*

national power. General Nakasone, the commander of US CYBERCOM and the director of the NSA stated in his confirmation hearings in March 2018 that *[b]y conducting operations to frustrate and counter adversary cyber activities to decrease will, increase cost, and deny benefits* (Sanger 2018). This illustrates that US CYBERCOM got an offensive mandate and an offensive mindset.

In the meantime, the Internet Research Agency continued to play a major part in the Russian disinformation campaign and remained active after the 2016 US Presidential Election which was being monitored by the US government. A month before the 2018 Midterm Elections on October 19, 2018, the DOJ indicted a Russian national for interfering in the US political system (Department of Justice 2018). The accused was charged for her alleged role in the Russian conspiracy to interfere in the US political system including the 2018 US Midterm Elections. The DOJ stated that *[u]nlawful foreign interference with these debates debases their democratic integrity, and we will make every effort to disrupt it and hold those involved accountable. The strategic goal of this alleged conspiracy, which continues to this day, is to sow discord in the U.S. political system and to undermine faith in our democratic institutions*.

In the meantime, US CYBERCOM were targeting the IRA's individual operatives and trying to deter them from spreading disinformation with aim of interfering in the 2018 Midterm Elections (Barnes 2018). US CYBERCOM's tactic was to tell the IRA's operatives that they have been identified and were being tracked in their work.

On election day, US CYVERCOM stepped up its game and struck the IRA directly (Nakashima 2019). Backed by intelligence from the NSA, US CYBERCOM blocked the IRA's internet access and thwarted the IRA's campaign of interfering in the 2018 US Midterm Elections (Moore 2019). US CYBERCOM's operations were the first offensive operations under their new objective given by the Pentagon. This offensive cyber operation was intended to prevent the IRA from disinformation aimed at undermining voters' confidence in the Midterm Elections and their outcome (Barnes 2019). The operation was aimed at taking the IRA offline for a couple of days so the voting results would be certified by local officials. According to the New York Times, the US Intelligence community had assessed that IRA was likely to step up its disinformation activity on voting day and while the votes were being counted (Barnes 2019). However, all was made public in late February 2019. Therefore, the general public was not aware that the IRA was continuing its disinformation campaign during the 2018 Midterm Elections.

Although the US, and US CYBERCOM in particular, stepped up their game, they did not engage disinformation on the level where the misleading information was present. The IRA's disinformation operations were targeting the information itself and made the quality of content contested. However, the US response was two-fold. They tried to influence the cyber troops by calling them out and they took down the infrastructure of the IRA. This last tactic was seen earlier in the way the NSA handled the online propaganda activities of terrorist organizations. US CYBERCOM used this 'old' tactic of taking something down for this new phenomenon of state-sponsored disinformation activities. Although this was an effective preventive measure for the future, it did not affect the previous actions at all. It seemed that the US had a limited toolbox when it came to engaging in foreign disinformation operations and engaging on the level of the information itself was not part of their toolbox.

5.6 Conclusion

Between the 2016 US Presidential Election and the 2018 US Midterm Elections, the Russian disinformation campaign became more clear. The investigation of Special Counsel Robert Mueller and the following indictment demonstrated the scale at which Russia tried to spread distrust towards the political system in the US.

The US government was aware that America's free and open political system was vulnerable to foreign interference. Russian tactics were not (only) aimed at compromising sensitive information and materials and interrupting critical services, they were creating division using legitimate means of social media. They used social media for their disinformation campaign via fake personas and controlled media outlets to inflame opposite ideological sides to further polarize the United States.

The US response to the Russian disinformation campaign was three-fold. First, they indicted several Russian nationals and organizations via their legal system. This created a public call-out to the Russian government. Secondly, they tried to influence the Russian cyber troops by letting them know that the US government was aware of their existence and their activities. Lastly, the US stepped up its digital posture tremendously. US CYBERCOM was given a new mandate, and this mandate was used to take down the IRA's infrastructure. However, these actions were not aimed against the misleading information itself. They were preventing further activities in the near future.

Chapter 6 Disinformation since the 2018 US Midterm Elections

The uncontrollable manifestation

The last two federal elections of the US were interfered with by Russian cyber troops seeking to sow division in the United States and they tried to spread distrust in the political system in general. The upcoming US Presidential Election was scheduled on November 3, 2020, and took place in the middle of a global pandemic. This pandemic has been highly politized and divided the society of the United States even more.

In this period information itself was becoming more and more contested. Correct and incorrect information became a matter of political opinion. Since information became objective and correct and false information resided in the same space, it was hard to make this distinction if it was even possible at all.

This chapter aims to answer the following question: *How is disinformation deployed in this phase, how is it perceived, and which attempts are made to mitigate the impact of disinformation?*

6.1 Information in a COVID-19 era

The 2020 US Presidential Election cannot be seen without the global COVID-19 pandemic. The pandemic outbreak reshaped the political, economic, and social systems in the United States (Johnson et al. 2020). The COVID-19 outbreak has been a rare occurrence for which there was no preparation. While the medical community was working to learn about COVID-19 including its symptoms, treatment, the spread of the infection, and the treatment of the virus for which there was no vaccine, the pandemic became politized. Political rhetoric was added to the messages of federal and state-level political leaders. The White House and its Virus Task Force tried to provide evidence-based information in a political setting. According to Johnson et al., the political rhetoric has at times emphasized a need to *get back to work* in the hopes that it will minimize the economic impact. This political desire is contrary to the advice of government actors concerned with the loss of life, thus creating political tension within and outside the federal government (2020: 252). In addition, the COVID-19 pandemic had a direct effect on the 2020 US Presidential Election which was held on November 3, 2020., because elections projections have not taken the vast loss of life into account which could lead to drastically shift in demographics of the voter base (Johnson et al. 2020: 253).

The global pandemic awakened the need for information. The demand for information to understand COVID-19, the effect it has on the healthcare systems, and many other unanswered questions about COVID-19 has created the perfect breeding ground for myths, disinformation, and conspiracy theories. While some can be dismissed as ludicrous and largely harmless, others are life-threatening (Fleming 2020). This breeding ground has triggered increased usage of social media platforms such as Facebook, Instagram, and WhatsApp by more than 50% during the lockdowns and social distancing period (Yang & Tian 2021). The use of social media led to an increase in information bubbles and echo chambers as seen during the 2016 US Presidential Election. Yang and Tian claim that the COVID-19 period was an information-rich environment that created illusioned knowledgeability and an optimistic bias against health disinformation.

6.2 Everything is contested

The 2020 US Presidential Election happened after two elections of foreign interference campaigns and during a highly polarized time in contemporary US history as a result of the global pandemic. These elections forced voters not only to form an opinion on the two Presidential candidates but also forced them to make a judgment about the integrity of the election process itself (Vail et al. 2022: 1). The US voters needed to judge whether Donald Trump or Joe Biden and their political parties might be likely to cheat and whether the integrity of the election would be threatened by voter fraud via mail-in ballots, ballot harvesting or foreign interference campaigns as seen in the past years. Voters also needed to judge whether they would accept the voting results as the outcome or that the other party might steal the election (Vail et al. 2022).

6.2.1 Free and fair elections?

Unique to the COVID-19 pandemic was the adoption of mail-in ballots since indoor voting stations were considered a public health hazard. Voting behavior indicated that Joe Biden would favor this type of voting. Donald Trump claimed that mail-in ballots would be rife with fraud from ballot harvesting, forgery, theft, illegal printing, and distribution to ineligible people. In turn, the Democratic Party became concerned that President Trump withheld funding to the US Postal Service and that Republican governors reduced the amount of official ballot drop boxes to one per county. Polls showed that limiting ballot drop boxes would disadvantage Joe Biden since his supporters were most affected by this decision. During the Presidential campaign, it became clear that acceptance of the voting results was at stake. For instance, Donald Trump refused to agree on forehand that he would accept the outcome of the 2020 US Presidential Election. The acceptance by the Democratic Party of the outcome was also uncertain due to their concerns about foreign interference. Both the Trump and Biden campaigns preemptively recruited lawyers for possible legal battles over the legitimacy of vote counts. This was a new phenomenon (Vail et al. 2022).

6.2.2 Election Day

Not all votes were counted at the same time. This depended on the method of voting. In-person votes were directly counted by the voting machines. The count of in-mail votes was only allowed after the polls were closed. Since most Trump voters voted in person and most mail voters favored Biden, meant that the forecast shifted drastically over time. The Swing States (Arizona, Georgia, Michigan, Nevada Pennsylvania, and Wisconsin) that led Trump to his 2016 victory, swung away from Trump and toward Biden. As the outcome shifted, Donald Trump cried foul about voter fraud and he began to reject the unfolding results of the election. He claimed, "*If you count the legal votes, I easily win. If you count the illegal votes, they can try to steal the election from us*" (Vail et al. 2022). Once Trump was likely to lose, his supporters strongly believed that it was the result of mail-in ballot fraud and they also began to reject the voting result (Colvin & Miller: 2020). Furthermore, Trump's base was increasing their support for resources against the outcome of the 2020 US Presidential Election. This included protests, legislative overhauls, legal challenges, destruction of property, and violence. Trump's legal team, led by Rudy Giuliani, began to file dozens of lawsuits in local, state, and federal courts, and even the Supreme Court challenging those counts (Shamsian & Sheth 2021).

When the press projected Joe Biden as the winner of the 2020 Presidential Election, Donald Trump refused to acknowledge this outcome nor did his supporters. His supporters continued to perceive fraud, therefore rejecting the election outcome, and supporting legal and violent means against it (Vail et al. 2020: 12).

6.2.3 The storming of the Capital

On January 6, 2021, US Congress scheduled a meeting to officially ratify Joe Biden as the winner (Vail et al. 2020: 12). At the same time, thousands of Trump supporters rallied in Washington D.C. and other state capitols across the country. In a public speech of President Trump, he claimed to have won the election and that it was necessary to stop the steal.

The first sign of this rally was on December 19, 2020 (Petras et al. 2021). On that day, President Trump tweeted about an upcoming rally in D.C. on January 6, 2021. Trump's *Save America Rally* began with speeches from his sons and then his main lawyer, Rudy Giuliani. Eventually, Trump himself started to address the crowd for more than an hour. In the meantime, lawmakers gather in the House of Representatives chamber on Capitol Hill. At the end of his speech, Trump returns to the idea of fighting for the country and urged those gathered in D.C. to walk to the Capitol. Trump stated "*We fight like hell, and if you don't fight like hell, you're not going to have a country anymore*," and he said. "*So we are going to walk down Pennsylvania Avenue – I love Pennsylvania Avenue – and we are going to the Capitol*." Not long after Trump's call, his supporters reached Capitol Hill and breached the police lines. This was followed by rioters climbing the walls of the Capitol. During the riots, Trump tweeted "*[Vice President] Mike Pence didn't dare to do what should have been done to protect our Country and our Constitution, giving States a chance to certify a corrected set of facts, not the fraudulent or inaccurate ones which they were asked to previously certified. USA demands the truth!*"

Over a thousand troops from the District of Columbia's National Guard were mobilized to support local law enforcement. Eventually, the rioters broke into the Capitol and the congressional leaders were evacuated from the area. In the end, over hundred forty law enforcement officers were injured during the riots and seven people died as a result. Three were Capitol Police officers and the four others were Trump supporters (Vail et al. 2020).

6.4 Conclusion

The 2020 US Presidential Election took place in a period where facts were not facts anymore. The global COVID-19 pandemic fueled the information bubbles and sow division in the society of the US even more than is already present. The health crisis was being politized and facts were called into question by alternative facts. All information was submitted to the question of *what is true and what is not true*. As a result, people answer this question based on their own beliefs and political preferences.

Distrust was fueled via social media and it became us versus them. In the end, there was no need for state-sponsored disinformation operations anymore. The suspicion towards the other political party, fueled by the media, and social media in particular created a setting where a legitimate voting process of a democratic country ended in seven dead and a storming of the Capitol. Disinformation manifested itself, it did not need guidance anymore.

Chapter 7 Analysis and conclusion

Disinformation in cyberspace did not start with the storming of the US Capitol because people believed the US 2020 Presidential Election was not fair and honest. It was a logical consequence of a series of events that started a decade earlier. Disinformation found its way into cyberspace and moved slowly in a direction that would affect the physical world. When that happened, disinformation has done its job of purposefully misleading its targeted audience.

7.1 Analysis

With the digitalization of modern society, cyberspace became more and more part of modern life. Although this development has created positive things, it also created new threats and exposed the vulnerabilities of a free and open society. The initial focus regarding the protection of cyberspace was on securing the information, maintaining the integrity of information, and keeping systems and digitalized processes available. At this point in time, the information itself was not contested. The US and other Western countries did not foresee that information itself would become a threat in the near future.

The first step towards contested information in cyberspace was propaganda that made its way into cyberspace. Various malicious non-state groups and organizations started to use the internet for propaganda purposes as if it were the offline world. The reaction of the US government was to monitor and occasionally websites were taken down by the authorities.

Time told that it took a couple of years until states shifted their offline propaganda activities toward the online world. Interestingly, when this happened, the phenomenon was no longer called propaganda, but it became known as disinformation to describe the use of cyberspace for spreading misleading information with the purpose of misleading.

It was during the 2016 US Presidential Election that state-sponsored disinformation campaigns saw the light for the first time. At the beginning of this election, the democratic party became the victim of Russian foreign intelligence (SVR) and military intelligence (GRU) hacking activities. The Russian operation shifted subtly since the GRU not only leaked stolen documents but also altered and manipulated these documents. If there is a birthplace when the propaganda became disinformation, this event marks that moment.

The Russian disinformation campaign created a situation that the United States did not foresee. In their perception, securing cyberspace was focused on the concepts of confidentiality, integrity, and availability. Russian activities demonstrated that the quality of the content and its originality were being contested as a result of disinformation operations. This was further amplified by the manipulative way political advertisements were being used and distributed amongst social media platforms. As a result, the US 2016 Presidential Election was the first time state-sponsored disinformation operations saw the light as a sole campaign instead of being part of a hybrid conflict and this election has shown the vulnerability of an open democratic society regarding (foreign) influence operations in cyberspace.

The United States investigated the matter extensively, and the Russian disinformation campaign that aimed to spread distrust towards the political system in the US became more

clear. The US government became aware that America's free and open political system was vulnerable to foreign interference. Russia's activities were not solely aimed at compromising sensitive information and materials and interrupting critical services. Their main tactic was to create division using legitimate means of cyberspace and in particular via social media. Once the United States understood the situation, their response was three-fold. The United States indicted several Russian nationals and organizations via their legal system, the US tried to influence Russian cyber troops by calling them directly, and they stepped up their digital offensive posture by giving US CYBERCOM a new and more offensive mandate. When Russia continued its disinformation campaign via the Internet Research Agency, US CYBERCOM took its infrastructure down.

At glance, this offensive operation looked groundbreaking. However, it is the same tactic used to tackle the online propaganda activities of malicious non-state actors and organizations. Not only are propaganda and disinformation used as a synonym, but the tactics of monitoring and taking down infrastructure were also copied. The US must have thought, if disinformation and propaganda are the same, the same solution can be used to counter it. However, new aspects that came with cyberspace such as the speed at which information is disseminated and the reach of online information were not taken into account by the United States.

Hence, the actions of the United States did not engage disinformation at the level of the information itself. So, people were informed that disinformation is a threat and disinformation is out there, but it is unclear what was disinformation and what was not. As a result, information itself was contested since everything could be disinformation or not. Labeling or framing of undesirable information as disinformation became part of the political division in the US.

By the 2020 US Presidential Election, Russia had already interfered in two federal elections. Furthermore, this election took place in a period where facts were not facts anymore. The global COVID-19 pandemic created even more information bubbles and continued to sow division within the society of the US. This global health crisis was also highly politized and facts were called into question by alternative facts. All information was submitted to the question of *what is true and what is not true*. As a result, people answer this question based on their own beliefs and political preferences. Distrust was fueled via various means and the United States society had become us versus them. The distrust towards the other political party created a setting where the legitimate voting process of a democratic country ended in seven dead and a storming of the Capitol on January 6, 2021. Disinformation manifested itself, it did not need guidance anymore.

The 2020 Presidential Election and its aftermath were the results of years of disinformation operations from Russia. Although it seems to be that they were not directly involved in sowing discord during this particular election, they laid the foundation for a divided and distrusted society. In the end, the Russian government succeeded in its objective of spreading distrust towards the US political system in general and the US failed to engage in disinformation on the level of information itself.

7.2 Reflection on the research

This research reconstructed a timeline of the transformation of disinformation in cyberspace based on the deployment, perception, and mitigation of disinformation in cyberspace. In this

process, four distinctive phases were identified which all had a different perception of the concept of disinformation and the appropriate responses to it.

Disinformation started as propaganda that made its shift from the offline world into the online world. Non-state groups and organizations used the advantages of the internet for their propaganda activities. The response of the US government in that period was to monitor the information and occasionally they took websites or other infrastructure down.

The second phase started when Russia conducted its disinformation operation outside of a hybrid conflict. During the 2016 Presidential Election, Russian cyber troops influenced the voting population of the United States and US society in general by spreading misleading information to mislead. Their goal was to sow distrust in the political candidates, and the political system of the United States in general.

The third phase started when the US was beginning to understand the impact of the Russian disinformation campaign. Various investigations by US congress and the US Department of Justice led to more understanding of state-sponsored disinformation operations. The US took a more robust posture and was getting ready to react to the Russian disinformation activities. On the day of the 2018 Midterm Elections, US CYBERCOM took down the infrastructure of the IRA that conducted the Russian disinformation activities.

The final phase in the transformation of disinformation is the uncontrolled manifestation of the concept of disinformation. This phase started after the 2018 US Midterm Elections and ended with the aftermath of the 2020 US Presidential Election, the storming of the US Capitol on January 6, 2021.

7.2.1 Limitations of the research

The focus of this research was on the significant disinformation events that took place, the insights that they brought, and the reactions to mitigate further disinformation threats. This research had three limitations. The first limitation is the scope of the research. It only focused on the interaction between the United States and Russia since this was these were the main actors involved in state-sponsored disinformation campaigns.

The second limitation is the direct implications of labeling a state-sponsored disinformation campaign, but not engaging on the level of the information itself. This research only looked at the indirect effect that caused a climate of contested information. It did not look into the concept of framing disinformation.

The final limitation is related to the second limitation. This research only investigated events that took place. Since there was no engagement on the level of information itself, this concept was not further explored.

7.2.2 Suggestions for further research

This research focused on the United States' response to disinformation. Although other states were not targeted by state-sponsored disinformation, they have observed what happened to the United States and learned from those events. It is the recommendation to research other countries and the European Union.

The final recommendation is related to the event that did not happen but perhaps could have had a mitigated effect of disinformation. The United States did not engage in disinformation on the level of the information itself. Disinformation makes advantage of the legitimate and

intended use of cyberspace with the intention to mislead the targeted audience. It is the auteurs' recommendation for further research to explore the concept of quality of content in addition to the classical concepts of confidentially, integrity, and availability.

References

Allcott, H. Gentzkow, M. (2017). *Social Media and Fake News in the 2016 Election*. The Journal of Economic Perspectives : a Journal of the American Economic Association., 31(2), 211–236. https://doi.org/10.1257/jep.31.2.211

Alperovitch, D. (2016, June, 15). *Bears in the Midst: Intrusion into the Democratic National Committee*. CrowdStrike. https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/

Aral, S. Eckles, D. (2019). *Protecting elections from social media manipulation*. Science (American Association for the Advancement of Science), 365(6456), 858–861. https://doi.org/10.1126/science.aaw8243

Bateson, R. Weintraub, M. (2022). T*he 2016 Election and America's Standing Abroad: Quasi-Experimental Evidence of a Trump Effect*. The Journal of Politics, 84(4), 2300–2304. https://doi.org/10.1086/718209

Barnes, J.E. (2018, October, 23). *U.S. Begins First Cyberoperation Against Russia Aimed at Protecting Elections*. The New York Times. https://www.nytimes.com/2018/10/23/us/politics/russian-hacking-usa-cyber-command.html

Barnes, J.E. (2019, February, 26). *Cyber Command Operation Took Down Russian Troll Farm for Midterm Elections*. The New York Times. https://www.nytimes.com/2019/02/26/us/politics/us-cyber-command-russia.html

Baumann, M. (2020). '*Propaganda Fights*' *and* '*Disinformation Campaigns*'*: the discourse on information warfare in Russia-West relations*. Contemporary Politics, 26(3), 288–307. https://doi.org/10.1080/13569775.2020.1728612

Bradshaw, S. Bailey, H. Howard, P.N. (2020) *Industrialized Disinformation: 2020 Global Inventory of Organised Social Media Manipulation*. Computational Propaganda Research Project. Oxford: Oxford Internet Institute.

Bradshaw, S. Howard, P.N. (2017) *Troops, Trolls and Trouble Makers: A Global Inventory of Social Media Manipulation*. Computational Propaganda Project Working Paper Series, Working paper 2017,12.

Brattberg, E. Maurer, T. (2018) *Russian Election Interference: Europe*'*s Counter to Fake News and Cyber Attacks*. Policy File. Carnegie Endowment for International Peace.

Chabinsky, S. (2009, November, 17) *Cybersecurity: Preventing Terrorist Attacks and Protecting Privacy Rights in* Cyberspace. Senate Judiciary Committee Subcommittee on Homeland Security and Terrorism. https://archives.fbi.gov/archives/news/testimony/preventing-terrorist-attacks-and-protecting-privacy-rights-in-cyberspace

Crilley, K. (2001*). Information warfare: New battlefields terrorists, propaganda and the Internet*. Aslib Proceedings, 53(7), 250–264. https://doi.org/10.1108/EUM0000000007059

Colvin, J., Miller, Z. (2020, November, 6) *Trump steps to the podium, baselessly attack election*. AP News. https://apnews.com/article/donald-trump-tweets-outrage-vote-count-df13d922b6249ff6c23d5021ae314e37

Department of Homeland Security. (2018, November, 5). *Joint Statement on Election Day Preparations.* https://www.dhs.gov/news/2018/11/05/joint-statement-election-day-preparations

Department of Justice. (2018, October, 19). *Russian National Charged with Interfering in U.S. Political System*. https://www.justice.gov/opa/pr/russian-national-charged-interfering-us-political-system

Director of National Intelligence. (2018, October, 19). *Joint Statement from the ODNI, DOJ, FBI and DHS: Combating Foreign Influence in U.S. Elections*. https://www.dni.gov/index.php/newsroom/press-releases/item/1915-joint-statement-from-the-odni-doj-fbi-and-dhs-combating-foreign-influence-in-u-s-elections

Fallis, D. (2015). *What Is Disinformation?* Library Trends, 63(3), 401–426.

Flaxman, S. Goel, S. Rao, J. M. (2016). *Filter bubbles, echo chambers, and online news consumption*. Public Opinion Quarterly, 80(S1), 298–320. doi:10.1093/poq/nfw006

Fleming, N. (2020). *Coronavirus misinformation, and how scientists can help to fight it*. Nature (London), 583(7814), 155–156. https://doi.org/10.1038/d41586-020-01834-3

Grinberg, N. Joseph, K. Friedland, L Swire-Thompson, B. Lazer, D. (2019). *Fake news on Twitter during the 2016 U.S. presidential election*. Science : a Weekly Journal Devoted to the Advancement of Science, 363(6425), 374–378. https://doi.org/10.1126/science.aau2706

Hankey, S. Marrison, J. K. Naik, R. (2018). *Data and democracy in the digital age*. The Constitution Society.

Hosaka, S. (2022*). Repeating History: Soviet Offensive Counterintelligence Active Measures*. International Journal of Intelligence and Counterintelligence, 35(3), 429–458. https://doi.org/10.1080/08850607.2020.1822100

Hunt, J. (2021) *Countering cyber-enabled disinformation: implications for national security*. Australian Journal of Defence and Strategic Studies. 3:1. 85-87.

Johns, F., Riles, A. (2016). *BEYOND BUNKER AND VACCINE*. AJIL Unbound, 110, 347–351. https://doi.org/10.1017/aju.2017.7

Jamieson, K. H. (2018). *Cyberwar: How Russian Hackers and Trolls Helped Elect a President*.

Johnson, A.F. Pollock, W. Rauhaus, B. (2020) *Mass casualty event scenarios and political shifts: 2020 election outcomes and the U.S. COVID-19 pandemic*. Administrative Theory & Praxis, 42:2, 249-264, DOI: 10.1080/10841806.2020.1752978

Jun, S.-I. (2016). *NATIONAL SECURITY OR PRIVACY*. AJIL Unbound, 110, 352–357. https://doi.org/10.1017/aju.2017.4

Lanoszka, A. (2019). *Disinformation in international politics*. European Journal of International Security, 4(2), 227–248. https://doi.org/10.1017/eis.2019.6

Marwick, A. Lewis, R. (2017) *Media Manipulation and Disinformation Online*. Data and Society.

Moore, M. (2019, February, 26). *US military blocked Russian troll farm's efforts to interfere in 2018 midterms*. New York Post. https://nypost.com/2019/02/26/us-military-blocked-russian-troll-farms-efforts-to-interfere-in-2018-midterms/

Mueller, R.S. (2018, February, 16). *Indictment Case 1:18-cr-00032-DLF*. Department of Justice. https://www.justice.gov/file/1035477/download

Nakashima, E. (2010, March, 19). *Dismantling of Saudi-CIA Web site illustrates need for clearer cyberwar policies*. The Washington Post. https://www.washingtonpost.com/wp-dyn/content/article/2010/03/18/AR2010031805464.html

Nakshima, E. (2019, February 27). *U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms*. The Washington Post. https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html

Nagasako, T. (2020). *Global disinformation campaigns and legal challenges*. International Cybersecurity Law Review, 1(1-2), 125–136. https://doi.org/10.1365/s43439-020-00010-7

Petras, G. Loehrke, J. Padilla, R. Zarracina, J. Borresen, J. (2021, February, 9). *Timeline: How the storming of the U.S. Capitol unfolded on Jan. 6*. USA Today News.

Rid, T. (2020). *Active measures : the secret history of disinformation and political warfare* (First edition).

Rogers, R. Niederer, S. (2019). *The Politics of Social Media Manipulation: A View from the Netherlands*. Netherlands: Eerste Kamer.

Rollins, J. (2010). *Al Qaeda and Affiliates: Historical Perspective, Global Presence, and Implications for U.S. Policy*.

Rosenstein, R.J. (2017, May, 17). *Appointment of special counsel to investigate Russian interference with the 2016 Presidential Election and related matter.* Department of Justice. https://www.justice.gov/opa/pr/appointment-special-counsel

Samonas, S. Coss, D. (2014). *THE CIA STRIKES BACK: REDEFINING CONFIDENTIALITY, INTEGRITY AND AVAILABILITY IN SECURITY*. Journal of Information System Security, (10)3, 21-45.

Sanger, D.E. (2018, June, 17). *Pentagon Puts Cyberwarriors on the Offensive, Increasing the Risk of Conflict*. The New York Times. https://www.nytimes.com/2018/06/17/us/politics/cyber-command-trump.html

Schia, N. N. Gjesvik, L. (2020). *Hacking democracy: managing influence campaigns and disinformation in the digital age*. Journal of Cyber Policy, 5(3), 413–428. https://doi.org/10.1080/23738871.2020.1820060

Schneble, C. O., Elger, B. S., Shaw, D. (2018). *The Cambridge Analytica affair and Internet-mediated research*. EMBO Reports, 19(8). https://doi.org/10.15252/embr.201846579

Schneier, B. (2016, July, 26). *The Security of Our Election Systems*. https://www.schneier.com/blog/archives/2016/07/the_security_of_11.html

Scola, N. Gold, A. (2017, October, 10). *Facebook: Up to 126 million people saw Russian-planted posts*. POLITICO. https://www.politico.com/story/2017/10/30/facebook-russian-planted-posts-244340

Shah, I. (1974). *The elephant in the dark*. Octagon Press Ltd.

Shamsian, J., Sheth, S. (2021, February, 22). *Trump and his allies filed more than 40 lawsuits challenging the 2020 election results. All of them failed.* Business Insider. https://www.businessinsider.com/trump-campaign-lawsuits-election-results-2020-11?international=true&r=US&IR=T

Schneble, C. O. Elger, B. S. Shaw, D. (2018). *The Cambridge Analytica affair and Internet-mediated research*. EMBO Reports, 19(8). https://doi.org/10.15252/embr.201846579

Splidsboel Hansen, F. (2017). *Russian Hybrid Warfare: A Study of Disinformation*. Dansk Institut for Internationale Studier.

Taylor, P. M.(2003) *Munitions of the Mind a History of Propaganda from the Ancient World to the Present Era* (Third edition).

Tenove, C. (2020). *Protecting Democracy from Disinformation: Normative Threats and Policy Responses*. The International Journal of Press/politics, 25(3), 517–537. https://doi.org/10.1177/1940161220918740

The White House. (2015). *The National Security Strategy of the United States of America*. https://history.defense.gov/Portals/70/Documents/nss/NSS2015.pdf?ver=TJJ2QfM0McCqL-pNtKHtVQ%3d%3d

The White House. (2017). *The National Security Strategy of the United States of America*. https://history.defense.gov/Portals/70/Documents/nss/NSS2017.pdf?ver=CnFwURrw09pJ0q5EogFpwg%3d%3d

Theohary, C. A. Rollins, J. (2011). *Terrorist Use of the Internet: Information Operations in Cyberspace.*

Trump, D. J. (2018, September, 12). *Executive Order on Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election.* The White House. https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-imposing-certain-sanctions-event-foreign-interference-united-states-election/

US Department of Defense. (2019). *2018 National Defense Strategy.* https://www.hsdl.org/c/2018-national-defense-strategy/

US Department of Defense. (2008). *2018 National Defense Strategy.* https://www.hsdl.org/c/view?docid=487840

Vail, K. E., Harvell-Bowman, L., Lockett, M., Pyszczynski, T., Gilmore, G. (2022). *Motivated reasoning: Election integrity beliefs, outcome acceptance, and polarization before, during, and after the 2020 U.S. Presidential Election*. Motivation and Emotion, 1–16. https://doi.org/10.1007/s11031-022-09983-w

Volkov, L. (2019). *How to Survive in Russian Opposition Politics*. The Fletcher Forum of World Affairs, 43(2), 57–66.

Wardle, C. (2017, February, 16). *To understand the misinformation ecosystem, here's a break down of the types of fake content, content creators motivations and how it's being disseminated*. https://firstdraftnews.org/articles/fake-news-complicated/

Whine, M. (1999). *Cyberspace-A New Medium for Communication, Command, and Control by Extremists*. Studies in Conflict and Terrorism 22, no. 3 (1999): 231–45. https://doi.org/10.1080/105761099265748

Yang, J. Tian, Y. (2021). *Others are more vulnerable to fake news than I Am: Third-person effect of COVID-19 fake news on social media users*. Computers in Human Behavior, 125, 106950–106950. https://doi.org/10.1016/j.chb.2021.106950

Zelenkauskaite, A. (2022*). Creating Chaos Online : Disinformation and Subverted Post-Publics*.