Alyssa J. Wilson

Combatting Disinformation Campaigns and Election Meddling: A Reappraisal of Strategic Communication

Master thesis

Prague 2019
Author: Bc. Alyssa J. Wilson
Supervisor: prof. Ing. Tomáš Karásek PhD.

Academic Year: 2018/2019
Bibliographic note


Abstract

In the context of increasing technologicalization and the growing interconnectedness of our world through social media, this thesis aims to answer the question, why is disinformation not being sufficiently handled in the United States in the wake of the foreign meddling in the 2016 Presidential Elections, and what can and should be done about the threat? This master thesis therefore aims to delve into the inherent vulnerabilities in the U.S. societal fabric, and thus conduct an in-depth explanatory case study model analysis of what should be done to further combat and counteract disinformation and election meddling within the country. The author argues that disinformation and election meddling are not only a serious security threat, but are also not being properly handled as they are only being addressed technologically, and not through the realm of information, and societal resilience. This thesis therefore argues that strategic communication, which should be redefined and expanded in definition, should be used to combat disinformation campaigns to prevent further election meddling. The author posits that a two-level approach is best, one which aims to negate the negative disinformation campaigns through a single governmental body, while also addressing the root causes through education.

Keywords

Strategic communication, disinformation, election meddling, United States, Russia, societal resilience, information warfare

Range of thesis: 60 pages, 116,464 characters
Declaration of Authorship

1. The author hereby declares that he compiled this thesis independently, using only the listed resources and literature.

2. The author hereby declares that all the sources and literature used have been properly cited.

3. The author hereby declares that the thesis has not been used to obtain a different or the same degree.

Prague May 10, 2019

Alyssa J. Wilson
Acknowledgements

An opus magnum of this magnitude and importance could not have happened without the support of many near and far. The first and heartiest of gratitude goes to Professor Tomáš Karásek, for his support throughout the process as both a mentor and a sounding board since the beginning. Thank you, Professor, for helping this idea to take shape and form, and for encouraging me to move forward with it, despite the many obstacles and obstructions along the way.

The next set of thank you’s goes to my fellow peers and cohort, for their unwavering support and steadfast belief. Thank you, particularly Daniela Santamaria, Natacha Cailler, and Tanya Demyanchuk, for always listening to the litany of worries, complaints, and successes throughout the journey.

Finally, and perhaps most importantly, thank you to my family, who buoyed up my spirits, willingly listened to the read-throughs of the drafts, and continued to support and have faith in me in my greatest moments of doubt. Though far away, I wrote this for you.
Combatting Disinformation Campaigns: A Reappraisal of Strategic Communications

Author: Alyssa Joy Wilson
Supervisor: Tomáš Karásek
Study programme: International Security Studies
Year of proposal submission: 2018/2019
Introduction

Disinformation campaigns have been the subject of much debate in the United States since the election of Donald Trump to office in November, 2016. Conjectures started flying about who actually elected the 45th President of the United States, was it Putin and his army of bots, or was it the disenfranchised American middle class? As speculation grew, the United States Congress, and then outgoing President Obama, condemned the Russian Federation for what he called, “the aggressive harassment of U.S. officials and cyber operations aimed at the U.S. election”\(^1\) and issued new sanctions as one of his parting gifts from the Oval Office. Such an incident shows us not only that disinformation campaigns were utilized as a part of a larger strategy to meddle in elections, but it has also left little doubt in security experts minds that disinformation campaigns are indeed a new form of threat, and should be taken seriously, given their larger implications. How to counteract it, however, is the dilemma. This thesis will thus address the question of disinformation campaigns, and how to classify them within the framework of international security. Instead of a minute threat posed through the growth of media and technology, disinformation campaigns need to be perceived as a direct attack on democratic societies, institutions, and on the current world order.

So what are disinformation campaigns and what do they achieve? How do they differ from propaganda, and, the greater umbrella term brought into security studies recently, strategic communications? Disinformation campaigns will be classified in this thesis as any sort of propagated information, news stories, or articles, through social or other forms of media, that are proven to be false, or at least partially untrue. It is important to note that while news stories that are only somewhat true may be spread without the intent of harm, or even without knowing that they are indeed false, disinformation campaigns are initiated by those who have an intent to undermine a democratic system through targeting emotionally salient issues, and can then be spread through ignorant, or apathetically unattached members of society. In the case of the United States, the “Russian troll factory,” as it is called in the European Parliament’s February 2018 report, was targeting high stake issues in the American context, such as race relations, immigration, immigration,

and gun control. These issues typically decide elections in the US, and most definitely define the bipolarity between the Republican and Democratic Parties. By targeting these questions, those spreading disinformation campaigns were targeting the weakest points of American society, in order to use a revised version of the divide et impera principle. The intent of spreading disinformation is therefore to showcase the weakest points of democratic societies, the divide on emotionally salient issues, and further increase divisions among the population in order to undermine democracy as a whole. This therefore showcases an inherent socio-political insecurity in the fabric of Western societies, which needs to be incorporated into the national security paradigm.

**Research target, research question**

This thesis will argue that the best way to do address this new insecurity, is to reformulate our understanding of disinformation campaigns, and how to combat them. Disinformation campaigns are a form of communication, and should therefore be treated, and reacted to, as such. Under a slightly different name, propaganda is fought with strategic communications. While propaganda and disinformation campaigns are not the same, when targeting democratic societies, they tend to have a similar purpose: to undermine democracy. Countering propaganda falls under the umbrella of Strategic Communications (which will also be referenced as StratCom), as it is the technique used to negate the effects of propaganda against the state. But why is propaganda fought with strategic communications, and the latter simple fact reports? Indeed, the European Union’s East StratCom Task Force, designed essentially in response to the spread of disinformation in Central and Eastern Europe, sees disinformation simply as a result of the populace having a lack of the facts. Therefore, their defense is designed along the lines of fact-checking. The research questions are therefore as follows: to what extent can StratCom be considered as, and applied to, countering disinformation? Additionally, how effective have we, as Western societies, been thus far in countering disinformation? If we have not been effective, in what ways could we use StratCom techniques, as applied to propaganda, to counteract disinformation campaigns?

---

The research target of this thesis is thus two-fold: first, it will be demonstrated whether or not countering disinformation campaigns falls directly under the jurisdiction of StratCom, and second, analyzing the efficacy, or lack thereof, of the techniques we have been using thus far, primarily fact-checking. The working hypothesis is that, given the emotions charged within the issues targeted, simple fact-checks and reports will not solve the problem. Instead, strategic communication is needed not only to understand and define disinformation, but also to combat it.

Theoretical/conceptual framework

Strategic communications (or simply, StratCom) and the development of its conceptualization has been propelled into the world of International Security in recent years. It has primarily been used, however, in the world of business to increase a company’s competitive advantage. This would indicate that StratCom is primarily used in the external promotion of a company, or, as has recently been discovered, of a state through its foreign policy. In recent years, however, information warfare, alongside the development and expansion of technology and social media, has led to new forms of threats in the Digital Age, as has been demonstrated in the 2016 elections of the United States. Strategic communications will be defined in this thesis as: any and all forms of communication with the intent of the promotion of the values of the state, whether it be as a defensive or offensive measure, designed to further strengthen the state’s positioning in the international world order. Within this definition, disinformation campaigns, and their elicited response, would then fall under the larger StratCom umbrella. As disinformation is a form of communication, effectively communicating and combatting them is best achieved through understanding their strategy, and effectively undermining it, which is what StratCom is designed to do. This thesis will prove, therefore, that combatting disinformation campaigns is a form of StratCom, which needs to be further developed and explored.

Methodology and data

For the first part of the research target, this thesis will deeply analyze, and conduct a close reading of, the current literature on strategic communication, in order to prove how combatting disinformation campaigns can be justifiably subsumed under the StratCom branch.
For the second part of the research target relating to the efficacy of current disinformation defense, this thesis will look at three cases of combatting disinformation. First, how the East StratCom Task Force of the European Union has been handling disinformation campaigns since its inception of 2015. The second case study will be the Czech Republic, and how it handled the disinformation campaigns during their Presidential Elections in 2017. The third and final case will be an assessment of the current measures being passed by the United States in light of the 2016 disinformation campaigns, which led to the election meddling in the Presidential Elections.

The selection of these cases has primarily to do with the volume of information on the cases, as well as the differing approaches of each organization or state. The East StratCom Task Force was created primarily to combat disinformation, and represents the intention of the EU to take disinformation campaigns seriously, and their incorporation of information warfare into their security paradigm. They also represent the strict fact-checking approach to combatting disinformation. However, the European Union is made up of several member states, thus, to get an even more in-depth approach as to how disinformation is conducted on the state level within the EU, the Czech Republic has been chosen as a case study due to the sheer amount of disinformation campaigns being conducted daily within the country, and because this thesis will be written partially on-site in Prague, giving easy access to security experts of the state. Finally, the US has been selected as the third case as a different kind of approach to disinformation defense, as they tend to focus on restricting social media platforms utilized by those spreading disinformation instead of interacting with the discourse, and because 2016 was the first case of such a large-scale information attack in the West, outside the European Union. The data needed to understand and interpret the efficacy of the various approaches will come primarily from academic articles, official government reports, and in the case of the Czech Republic, interviews with experts in the information warfare and security field. In order to assess the efficacy of the approaches, this thesis will primarily focus on two variables: the scope of the audience of both the disinformation, and the consequent defense; and the length of the news cycle for the story, both the false information, and then the corrected information. These variables were chosen in order to showcase how widespread the disinformation campaign was, and then how many people the state or task force reached with the correct information. The news cycle’s length can demonstrate how prevalent it was to the population’s decision-making around the time of key democratic elections. Given the spread of the disinformation in Europe, and more specifically, the Czech Republic, it
would be nearly impossible to know exactly how many people may have been swayed to vote a
certain way by one disinformation campaign, not to mention that understanding the decision-
making process of individuals is a herculean, if not impossible, task at best. This thesis instead
will work under the assumption that the mass media cycle, its length, and its scope, loosely
represent the breadth of the disinformation campaign’s reach and affect.

**Planned thesis outline**

The preliminary structure of this thesis will be as follows:

- Introduction
  - Disinformation defined and its characteristics
  - Disinformation campaigns as a part of election meddling: the shift towards insecurity and the thesis motivation
- Chapter 1: Conceptual/Theoretical Framework
  - Strategic Communications defined
  - Communications theory
  - Methodology: case studies
- Chapter 2: Combatting disinformation, redefining strategic communications
- Chapter 3: Case studies, how effective is the West in countering disinformation?
  - EU East StratComTask Force
  - Czech Republic
  - US
- Conclusion/policy recommendations for countering disinformation

**References and further reading**

https://euvsdisinfo.eu/disinformation-cases/?offset=0.


Contents

INTRODUCTION .................................................................................................................. 16
THEORIES AND METHODS .................................................................................................. 19
  1. Strategic Communication
  2. Information Warfare and its Toolkit
  3. Single Case Study: The Thesis Methodology

PRIMARY CASE STUDY: THE UNITED STATES ......................................................... 33
  1. The Russian Troll Factory, Cambridge Analytica, and a Divided Population: The 2016 and
     2018 U.S. Elections in the Battle for Public Opinion in the U.S. Information Space
  2. Background on U.S. Information Institutions, and the Evolution of Strategic Communication
     Meddling, and Encourage U.S. Societal Resilience

CONCLUSION .................................................................................................................... 55

BIBLIOGRAPHY ............................................................................................................... 57
Introduction

In 2016, then U.S. Presidential candidate Donald Trump infamously codified any media source which did not agree with him, or portrayed him in an unflattering light, as “fake news.” This simple phrase spread like wildfire throughout the country, and today remains the colloquial term for all manner of negative communications, including propaganda, libel, and even disinformation campaigns. Ironically enough, however, very little attention was paid by the public to the subtle disinformation influencers and bots on social media during the U.S. Presidential Elections of 2016. In the aftermath of the drawn-out face-off between Hillary Clinton and Donald Trump, some experts raised the alarm by noting the election meddling and minutiae of disinformation campaigns which had been spread during the fall, however, disinformation as such was not codified to be a threat among security experts until nearly two years later, when more reports came out about the extent of foreign meddling in the U.S. elections.

Just a year prior, in March 2015, the European Union created the EU External Action Service East StratCom Task Force. According to its website, it was set up to combat Russia’s disinformation campaigns going on throughout the European Continent.3 The EU External Action Service (EEAS) maintains three main objectives concerning the Task Force. First, it wishes to “maintain effective communication and the promotion of EU policies in the Eastern Neighborhood.”4 Second, it aims for the “strengthening [of] the overall media environment in the Eastern Neighborhood and all EU Member States, including support for media freedom and strengthening independent media.”5 And finally, it strategizes an “improved EU capacity to forecast, address and respond to disinformation activities by external actors.”6 Overall, the East StratCom Task Force is well endowed to address the information warfare being waged throughout the continent through disinformation campaigns.

Instead, the U.S. approach has been to combine disinformation, propaganda, and maligned information warfare being waged outside the United States all under one category, to

---

3 For more information, see EUvsDisinfo, https://euvsdisinfo.eu/about/.
5 Ibid.
6 Ibid.
be taken care of by the Global Engagement Center (GEC) in the U.S. State Department, while domestically, it has no single body, and is instead split between private industries, the Department of Justice, and the Department of Homeland Security. More disturbing than grouping these malign influences together, and the red tape separating what happens externally from what happens internally, is the aim of the GEC toward codified non-state actors. The organization, created in April 2016 and drafted into law a year later,7 is “charged with leading the U.S. government’s efforts to counter propaganda and disinformation from international terrorist organizations and foreign countries.”8 However, the disinformation campaigns and further election meddling in 2016, and the attempts made in 2018, were not led by terrorist organizations, but by a small group of actors that cannot be definitively tied to a government through clever means of plausible deniability. As will be explained in further detail, the election meddling carried out in the United States was skillfully handled by a coordinated effort on the part of many individuals, some of whom have already been prosecuted or indicted.9 More importantly however, is that the emphasis placed on terrorist organizations negates a whole gamut of people who are known to be malign influencers, and a whole new threat category, which appears to have gone unnoticed, despite the United States’ prior history with information warfare coming from the Soviet Union.

Such a lack of preparedness, and a continued lack of sincere counteraction to the threat, leads to a gap in the national security paradigm, one which is slowly growing and becoming more threatening each year, and with each new social media account added. This begs the question therefore, why is disinformation not being handled sufficiently, and what can and should be done about the threat? This master thesis therefore aims to delve into the inherent vulnerabilities in the United States’ societal fabric, and thus conduct an in-depth analysis of what should be done to further combat and counteract disinformation and election meddling within the country. This analysis will be conducted based on the results of an explanatory case study model, as explained in Pamela Baxter and Susan Jack’s 2008 article from The Qualitative Report.10

---

8 Ibid. Emphasis my own unless otherwise stated.
author argues that disinformation and election meddling are not only a serious security threat, but are also not being properly handled as they are only being addressed technologically, and not through the realm of information, and societal resilience. The next few chapters will thus argue that strategic communication, which should be redefined and expanded in definition, should be used to combat disinformation campaigns to prevent further election meddling.

First, in the Theories and Methods chapter, key concepts such as strategic communication and disinformation will be defined in order to best understand how to utilize the former to combat the latter. In the Case Study chapter, the background on the election meddling conducted during the fall of 2016 will be assessed for weakness and the vulnerabilities being targeted, in order to best analyze a counter-strategy, and to provide the necessary context to understand the extent of the threat the United States is facing. The chapter will then go on to discuss the evolution of information institutions in the United States, and how strategic communication has previously been used and defined domestically. Finally, the chapter will conclude with what the author believes to be the most effective ways of counteracting disinformation and election meddling: a two-pronged approach that aims to both negate the disinformation through a single governmental body, and courses in education to effectively address the root causes of the lack of resilience against, and understanding of, information warfare. The thesis will conclude with a brief summary of the main arguments, and a widening of the possible future threat.
Theories and Methods

As previously mentioned, this chapter will outline the key theories of this thesis, beginning with how to define strategic communications itself, including a brief literature review of the discipline, and then its evolution within U.S. institutions. Subsequently, supplementary concepts will be discussed, primarily focusing on disinformation campaigns, and their connection to election meddling. For the sake of clarity, propaganda will also be defined, as there are those who seek to disguise their malignant intentions under the guise of strategic communications.

1. Strategic Communication

Strategic communication (also referred to as stratcom) has primarily been viewed by two academic schools of thought: those who focus on the strategic and those who focus on the communication. This thesis will do both, since it will be argued that the concept of stratcom should be—and to a certain degree has already been—coopted by the realm of international security. However, to get a better sense of the concept, a brief, and therefore narrow, literature review is in order to understand the definition at large.

Strategic communication has largely been used as a tool in the business world. For several decades now, one could find the word “strategy” or “corporate communication strategy,” in books, articles, or even courses about business and entrepreneurial endeavors. However, strategy as such was ill-defined, as noted by Benita Steyn in 2003. Hallahan et al. in their 2007 article, “Defining Strategic Communication,” stated “defined in its broadest sense, [strategic communication means] communicating purposefully to advance [the organization’s] mission.”

In their article, stratcom is a discipline, a larger, overarching umbrella under which all other communication of an organization rests. Marketing, management, advertising, and public relations all fall under the discipline so long as they are geared toward advancing the organization’s mission.

---


There is much debate among scholars on what exactly stratcom is, let alone its purpose. If we are to believe that strategic communication promotes the ideals and values of a company in line with set goals, is the strategizing of said goals incorporated in stratcom, or is stratcom only the furthering of these marks of success? Hallahan et al. along with Thorson (2013) fall into the former category, maintaining that defining the strategy of the company, then pursuing it through various avenues of communication constitute strategic communication. Holtzhausen and Zerfass (2015), on the other hand, believe stratcom’s duties begin after the strategy of the firm has been confirmed, and that any communication with the intent of buoying up such prospects defines strategic communication. For the sake of this thesis, strategic communication will constitute the promotion of the various ideals and values of the government, as the strategy is handled by a number of agencies, numerous cabinet members, and often does not overlap with the communicative aspects of the strategy.

Since Hallahan’s 2007 article, there has been much debate on how broad—or how narrow—strategic communication really is. Unlike newer authors such as Nothhaft and Schlözel, Hallahan et al. focus on the communication of strategic communication, rather than the strategic. Naturally, there is also much debate about what communication actually means. In 1983, Littlejohn posited that communication theory “refers to the body of theories that constitute our understanding of the communication process.” Littlejohn also maintains that theories, as abstractions, mean they are only partial in their completion, indicating that there is a conglomeration of theories needed to understand communication as a whole. This is where further disagreement occurs, in order to understand and determine which aspects should be considered as crucial, or of lesser importance, when trying to ascertain the exact art of communication. Lasswell (1948) focuses on who does what and to what effect, while much

---

17 Van Ruler, “Communication Theory…” 367.
18 Ibid.
more recent schools of thought focus on meaning creation, and how interaction and socialization can be attributed to such a phenomenon.\textsuperscript{20} Meaning creation is generally accepted today as the main function of communication; by indicating or referencing a certain object, then naming it, and whether or not the audience accepts it, the referent object has been named, and the meaning of the word used created. There is, naturally, additional disagreement as to whether or not such meaning creation is a linear one-way process, a two-way process, or a multi-linear diachronic process, in which the constitutive belief is that meaning comes about through a process of socialization between multiple actors over time, and is in a constant state of evolution.\textsuperscript{21} As is evident, these debates are in no way resolved or truly finished, so for the case of this thesis, we will assume that communication falls into the latter category of a diachronic, constitutive, fluid process that comes about through socialization with multiple actors at various times.

In shifting focus from \textit{communication} to \textit{strategic}, Nothhaft and Schölzel (2015) on the other hand, turn to the forefather of strategy, Carl von Clausewitz, to assist in defining the term. In his famous work “On War” (1832), Clausewitz notably compared war to commerce, stating that instead of art, “war […] is a conflict of human interests and activities.”\textsuperscript{22} On strategy, he identifies three general imperatives according to Nothhaft and Schlözel. First, is the capture of public opinion, second is the destruction of the hostile army, and finally, the seizure of its resources and means.\textsuperscript{23} Clausewitz also noted,

The first, the supreme, the most far reaching act of judgement that the statesman and commander have to make is to establish […] the kind of war on which they are embarking; neither mistaking it for, nor turning it into, something alien to its nature. This is the first of all strategic questions and most comprehensive.\textsuperscript{24}

\textsuperscript{20} Van Ruler, “Communication Theory…” 368.
\textsuperscript{21} Ibid, 374.
The authors Nothhaft and Schlözel remark, however, that the concept Clausewitz is trying to convey is both vague and concrete at the same time, much like it is today in the management discourse, unlike, Hallahan et al. in their 2007 article, who cut through all ambiguity.

Such differences in opinion are difficult to overcome in the scholastic world, but as mentioned previously, this thesis must consider both aspects of the definition: the strategic for its security implications, and the communication for the new tool of defense. While Nothhaft and Schlözel made the case for stratcom to be observed in Clausewitzian terms, we must go further. As will be demonstrated in the second section of this chapter, words are a tool of war that is being adeptly used in the 21st century. Though information warfare is not necessarily new, the execution is now being remodeled with the onset of new technology, and the birth of social media. The need for stratcom to be expanded to observe not only the strategic aspect, but also the communication, is essential in order to best address the vulnerabilities we in the West share when facing information warfare, both from within, and without. Strategic communication is not simply a tool to be used in international security because of the Clausewitzian definition of strategy, but it is of further importance because of the newest threats we are facing. With this in mind, strategic communication in this thesis will be defined and expanded as a tool which both promotes and defends the mission of the State, both domestically and abroad, to capture the public opinion in the war of information being waged through disinformation. Strategic communication will be treated, similarly to Hallahan et al., as a larger umbrella under which multiple things fit, including both domestically-geared, and internationally-focused principles. To further extrapolate, the author maintains that stratcom can be separated into both proactive and reactive forms: the former to actively promote certain aspects of U.S. life or its political approach and values; and the latter as a reaction to negative information campaigns. In addition, both of these can be used to differing degrees both domestically and abroad, and some are actively used in certain departments of the U.S. Department of State (as will be further shown in the following section). The author believes that in expanding the definition of stratcom, we can also hopefully begin to see which parts are missing, and better address the information war we are currently waging.

---

25 Nothhaft and Schlözel “(Re-) Reading Clausewitz…” 21.
2. Information Warfare and its Toolkit

Before we can truly define information warfare (IW), one should evaluate how it is that we got to this point. As the RAND Corporation pointed out in their exposé, “Strategic Information Warfare: A New Face of War,” IW is the product of a larger trend named the information revolution. The revolution has expanded due to a growth in information technology, cyberspace, and even, the author would argue, an evolution in the way we think and consume information around us. With computers being accessible to the majority of the world’s population—57% as of January 2019—and with social media now being used by 3.84 billion people worldwide (45% of the world’s population), such an explosion onto the world stage of these new mediums have clearly changed the way we interact with our communities, our world, and especially, the information we are exposed to daily. In the past year alone, social media and internet users worldwide increased by 9% each. In the Western World internet penetration hovers at 95%, with on average, 65% of Western populations as social media users. It is therefore reasonable to assume that what happens on the internet and social media will have a fairly substantial impact on Western societies. With such a growth and impact of social media being evident, it is understandable that it can also be a source of vulnerability in today’s societal fabric. Information warfare, therefore, is a phenomenon rising out of the growth in internet users and increasing technological capabilities around the globe, and can be defined as the intentional use and manipulation of information, both truthful and falsified, and rhetoric to gain an advantage over a perceived adversary by targeting weaknesses, vulnerabilities, and divisions in its societal fabric.

There are several notable aspects to this definition. Important to note first is the word intentional manipulation of information. News stories, status updates, and posts are uploaded constantly on social media and the internet, but it is the choice to twist, to spin the story that propels this into the realm of warfare, because it is the intent that shows the desire to weaken an

---

28 Ibid.
29 For this thesis, the Western World will be defined as NATO and EU allies unless otherwise stated.
30 Chaffey, “Global social media research…”
opponent. Second is the emphasis on truthful and falsified. If the information is false or made to be untrue through manipulation of the story, then it falls into the realm of disinformation, which will be highlighted later in this chapter. But, a story does not have to be false to be manipulated. It could be leaked, shared with the public, as with the Wikileaks incidents, or revealed prematurely. Finally, and possibly most crucially, one should note the vulnerabilities and divisions that are targets of information warfare. Information warfare is used to further divide, to weaken societies, which shows our shift in our security paradigm from simply physical and national security, to human security. The case of the U.S. 2016 presidential, and to a certain extent, 2018 midterm elections will further demonstrate the effects of astutely waged information warfare in the next chapter.

As was previously highlighted, disinformation derives from the falsifying of information in order to sow chaos and divisions in an adversary’s society. However, once again, intent changes everything. Stories get redacted; journalists, newscasters, and writers misrepresent information often, but this is not to be confused with disinformation, so long as there was no intention to do harm or to misrepresent the truth. While intent is extremely difficult to prove, and therefore barely subject to falsifiability, disinformation, when linked to election meddling, can show both malicious intent and harm, and a sense of warfare. Disinformation is therefore defined in this thesis as the falsifying of information for gain, whether that is to create chaos, or in the interest of manipulating an adversary’s population’s emotions toward a series of actions that will produce an outcome more favorable to your own interests than your adversary’s. The creation of chaos is an important aspect, because many authors have argued recently that actors like Russia seek to create chaos so that autocratic rule is more easily perpetuated, and to destabilize Western society, which they perceive to be an adversary.\(^\text{31}\) Aside from intent being the operable paradigm, the other key words in the definition are the manipulation of a population’s emotions and actions. As was already mentioned, information warfare aims to divide, and disinformation is therefore most successful when there are issues which already create divisions and disagreements among members of a society, and which are deeply rooted in certain values, ideals, or other emotional forms of attachment. The more that a certain disinformation campaign

---

is propagated, the more heightened the emotions around a certain issue of importance become, which can lead to more protests, uprisings, and other disturbances.

Disinformation alone is of concern in the security world, given its ability to stir certain actions out of members of a population, but the aspect most disturbing is its linkages to election meddling, which roots it firmly in the world of international security. Governmental elections are an inherently sovereign and sacred act between the people of a nation and its elected officials. It is a form of social contract, a promise that the power and determination of the direction of a country lies firmly with its citizens, a pact enshrined since the American and French Revolutions. While the practice has evolved and expanded throughout the past three centuries, the basic premise remains the same: the decision of who should run a country, how it should be done, and in what direction it should go in, rests with the people of a nation-state. These people do not have to be within the country at the time usually, but it is a sovereign act; typically, only those with a citizenship of the country can vote. In its basic presupposition, elections are sovereign, no other nation or national has the ability, nor the right, to decide its outcome, even if a particular ending would suit their own interests for better or worse. While elections are an inherently sovereign institution, they are also a time of great transition, and transition periods are when a society, and by extension, its government, are at their most vulnerable. This is why during coups, or after a monarch died, it was imperative that the secession be established well in advance, so as not to further induce chaos into who should rule the realm. Elections are no different; representing a period of uncertainty and transition, elections are the time in which democracies are at their most insecure and vulnerable, which therefore makes them a logical target in the new realm of security. When coupled with the technologicalization and digitization of elections, ballots, and voting, elections are therefore an easy target in the world of information warfare. As will be expanded upon in the next chapter, election meddling posed a great risk to the U.S. presidential and midterm elections in 2016 and 2018, and in many ways appear to have altered the results in favor of those behind the meddling: Russia.

While the precise link between disinformation and election meddling is not entirely clear, it can be drawn in a couple of ways. First, disinformation campaigns are simply one of the tools which can be found in the toolkit of election meddling. Just as elections are supposed to bring together a population to decide upon a new course and direction for their country, disinformation is meant to divide and separate, causing greater rifts and chasms among people who should be
heading toward a common goal, but who continue to find themselves on opposing sides. Disinformation, through social media and using particular techniques and algorithms, deepen the divide and further separate people, which may not itself inherently result in changing a person’s mind on an issue being debated in the elections, but it does allow for a lapse in empathy for other’s opinions. Once that lack of empathy, or even remote understanding, for other points of view is planted, it is easier to distinguish between “us” and “them,” a classic “othering” technique. In creating such divisions, a society can lose a common ground, and when losing common ground, you lose a certain set of universal truths and beliefs, and it is exactly this disengagement from truth and belief that disinformation profits from.

One key question though is, why meddle in the elections to cause chaos? There are many different possible targets that those challenging the status quo could use. While it may appear obvious, it is important to unveil exactly what makes elections a prime target in the new age of information warfare and hybrid warfare. Elections are a time of transition in democracy. They are the times when the system is at its most vulnerable because it represents a transfer of power, one which is generally venerated by those who promote democracy because it represents the freedom to choose by the electorate, and a peaceful transition of power is often a symbol of pluralism in government, noted as a key indicator of how “free” a country ranks, according to Freedom House. However, elections are not only crucial, but they are a time of great confusion, and the greatest vulnerability, since the votes determine who will be in charge and governing the country and its policies for the next few years. As that is the heart of the power, and the heart of the democratic political machine, it is understandable that it would be seen as a target. In addition, as elections move toward being electronic and used through technology, they are subject to even more vulnerabilities as cyber capabilities of countries increase.

In relation to election meddling however, disinformation is used primarily to cause confusion and chaos. Election meddling is defined as the act of disregarding the sovereignty of elections and trying to tip the scales in favor of your own interests. In the case of the U.S., dividing people and making them not trust in the news because it does not align with the “truth” they previously believed, and such resulting chaos is one way to meddle in the elections because of its ability to change people’s voting pattern, or more realistically, get them to not vote at all.

---

Once you have divided the electorate, adding in disinformation campaigns creates more confusion, and supplements the overall meddling.

If we focus on Russia as the main perpetrator, in the case of the United States, then it is important to note that each target and each election is handled differently by the Kremlin; there is no single one-size-fits-all method. This is of the utmost importance when creating a counter-strategy, which will be discussed near the end of the case study chapter. In 2016, the Center for Strategic and International Studies (CSIS), based in Washington DC, published their work called *The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe*, in which they outlined the key strategies of Russia in several countries across Europe, including the various tools in the information warfare toolkit.33 Despite the title, the book notes that while some of the tools may remain the same, there is no single way to meddle in an election, and the tools being deployed are dependent on various factors within in the target country. According to the authors, “While there are specific patterns of conduct within each track, there is no clear-cut path that Russia appears to follow in any case. Rather, a tactical combination of actors and drivers may be used in pursuit of specific strategic outcomes—all of which depend on the unique conditions present within each country, thus acquiring a Russian “tailor-made” strategy.”34 Furthermore, the authors go on to argue,

Russian influence centers on weakening the internal cohesion of societies and strengthening the perception of the dysfunction of the Western democratic and economic system, which has stagnated since the global financial crisis and reels from the effects of globalization. This is achieved by influencing and eroding democratic governance from within its own institutions.35

Aside from disinformation, there is a large range of strategies, or tools, that are employed. According to the playbook, Russia employs two main tracks, not mutually exclusive, but in fact mutually reinforcing in an un-virtuous cycle: an economic track, “aimed at manipulating a country by dominating strategic sectors of its economy[…]” and a political track, that “seeks to corrode democracy from within by deepening political divides and cultivating relationships with aspiring autocrats, political parties (notably nationalists, populists, and Euroskeptic groups) and

33 Conley et al., *The Kremlin Playbook*...
34 Ibid, xi.
35 Conley et al., *The Kremlin Playbook*… xii.
Russian sympathizers.”36 Although CSIS’s publication focused on five Central and Eastern European countries, Hungary, Slovakia, Bulgaria, Latvia, and Serbia, there are a number of parallels in terms of the goals of the Kremlin that can be found in the case study of the United States, all of which will be flushed out in the next chapter. Notably, this thesis will focus on the latter, politically-directed track, as that is primarily what describes Russian malign influence in the U.S. elections and the consequent meddling. These two tracks take on unique features in each country depending on the political and economic climate, however, there are some general features which can be found, and which have been described in the Playbook. Typically, the economic influence begins first, with a quiet, opaque Russian network of businessmen making seemingly legal deals with local entrepreneurs and company owners, and over time their grip tightens on various industries, including but not limited to energy, finance, media, and infrastructure.37 As Conley et al. explain, Russian malign influence is like a “virus that attacks democracies […] penetrating a country […]”38 These economic transactions happen without the so-called host of the virus knowing, and continues its political and democratic system as normal. However, over time, the host economy becomes so compromised that the precise steps taken to prevent corruption and monopolies become ineffective. If the public resists through democratic or political means, the host government could then be exposed through the media to show the extent of the corruption, which can render the host government illegitimate.39 In so doing, the Kremlin has also fostered anti-European or anti-American sentiment by furthering the divide presumably being showcased between the democratic system, and those who seek to elect it, the people. According to the Playbook, “there is an undeniable elegance to these “win-win” tactics for the Kremlin; it is the perfect strategy to erode the foundations of democracy from within and discards the Western model of governance, while elevating the Kremlin’s.”40 As can clearly be seen, the erosion of democratic values through the exposure of corruption directly correlates to that which happened in the 2016 presidential elections in the United States, and will be further elaborated upon in the next chapter.

36 Ibid, xi.
37 Ibid, xiii.
38 Ibid.
39 Conley et al., The Kremlin Playbook… xiii.
40 Ibid, xiv.
One more note that must be made is that election meddling, at its very basic form of designing a transfer of power favorable to your own interests, is not new. Disinformation, and its consequent spread through society to create chaos, foster divisions, and plant confusion and mistrust, is also not new. If one removes the technological aspect of both election meddling and disinformation campaigns, one would recognize it as a tale as old as politics, noting that in the realist school of thinking, states have always attempted to sabotage their perceived adversaries by any way possible, including inspiring coups or a transfer of power to someone more sympathetic to your cause, or spreading false information in the hopes that society will turn against its current leaders, or become apathetic to the cause. Nevertheless, election meddling and disinformation in the new age of globalized technology and an inter-connected world through social media webs and entanglements has created a new security and threat nexus which can no longer be ignored, or deemed “old news.” Our lack of understanding of just how social media works, both technically and socially, is only to society’s detriment, and further increases our inherent vulnerability through our inability to comprehend the threat we are facing.

Though our lack of understanding of technology has been to our detriment, we must also recognize that there is another component to our slow reaction to the threat of information warfare, and it can be attributed to a case of political and security amnesia, in which we seemed to forget that information warfare is a tool of war, one which the United States should be familiar with, especially coming from the Russian Federation, previously the Soviet Union. The USSR during the Cold War was no stranger to information warfare, and a war of words through propagandistic, malign influences. However, after its collapse, it went through a period of dormancy as it dealt with its internal struggles, including the implosion of what had been a federation of republics for more than seventy years. The focus of U.S. foreign policy, and in turn that of the academic world and security experts, then shifted to the Balkans, an area torn by war and chaos that threatened other European allies, and the Gulf states, as a battle for influence was waged, among other concerns of the 1990s. Not to mention, that after 9/11, the main focus of the security community has been on terrorism, and issues of securitization and exceptionalism, while hybrid warfare, including the war of words, has only recently returned to our academic consciousness. Propaganda and information warfare therefore took a backseat in the forefront of foreign policy, however, when it was revived under President Vladimir Putin, there it seemed to be a lapse in memory, and the West suddenly found itself facing the threat as if it had never seen
it before, which is clearly a fallacy. Such thinking negatively affects our ability to best respond to the threat, as instead of drawing upon our previous experience, we have been treating the threat as if it is entirely new, rather than an extension of—a continuation of—a larger Russian foreign policy tool, that merely went dormant for a decade or two. One distinction that should be made is between propaganda and disinformation, and strategic communication, as there are many who wish to purposefully confuse the notions in order to justify their own actions, or redefine their policies. Propaganda can be defined as “a form of communication that attempts to achieve a response that furthers the desired intent of the propagandist.”41 This being a generally vague definition, the author portends that propaganda can generally also be noted for its truthful undertone, with the hope of a certain outcome, differing from disinformation in that the latter aims to purposefully mislead readers or consumers in order to result in a certain action. If something cannot be proven counterfactually, if something is thus considered to be untrue, and if the actors’ motivation is to influence the outcome of a certain situation, then it can be distinguished as disinformation. Propaganda is also used by states to promote their culture abroad, as a form of soft power, sometimes called Public Diplomacy, which will be further discussed in the next chapter. Furthermore, strategic communication is not necessarily adopted with the intention of a certain action, more with the hope that the company, or in this case a government, will be seen more favorably. While a thin line, these concepts are unfortunately not mutually exclusive, and there is a distinction that should be made.

3. Explanatory Case Study: The Thesis Methodology

As was stated in the introduction of this thesis, its secondary purpose is to understand the breadth and width of the disinformation and election meddling that took place in the United States in 2016, and the attempt in 2018, in order primarily to best assess the vulnerabilities the U.S. is facing when strategizing a plan of counteraction. In order to soundly analyze the case study of the United States in the context of election meddling and disinformation, a firm grounding in methodology is needed in order to establish any sort of legitimacy of the following research.

The methodology that was selected for this thesis is an explanatory case study, as described by Baxter and Jack in their 2008 article, “Qualitative Case Study Methodology: Study Design and Implementation for Novice Researchers.” According to them, a case study “[…] is an approach to research that facilitates exploration of a phenomenon within its context using a variety of data sources. This ensures that the issue is not explored through one lens, but rather a variety of lenses which allows for multiple facets of the phenomenon to be revealed and understood.” In the context of this thesis, there are several factors which will be taken into consideration, including the key themes highlighted in election meddling and the social media campaigns, which appear to have the most salience in U.S. politics for the time being, in addition to the larger historical and social context of the U.S. political and democratic system and its institutions.

Baxter and Jack also posit that a case study approach should be considered when “[…] (a) the focus of the study is to answer “how” and “why” questions; (b) you cannot manipulate the behavior of those involved in the study; (c) you want to cover contextual conditions because you believe they are relevant to the phenomenon under study; or (d) the boundaries are not clear between the phenomenon and context.” This case study certainly falls under each of the individual justifications. Not only has the phenomenon happened in the past, therefore inhibiting the study or manipulation of those involved, but also context is essential to understanding how and why certain issues were targeted during the elections as the conjunction of disinformation and social media posts. The research question of this thesis aims to determine the impediments to combatting disinformation in the United States, and what the vulnerabilities are among the population that need to be reinforced in order to secure the state against future meddling, which is situated between a “why” and a “how” question. Finally, the boundaries are blurred between the phenomenon and the context, because the salient issues being discussed during elections are not linear, but instead more akin to a cycle, as they are constantly developing and changing throughout the timeline of an election, including how they are discussed rhetorically.

According to Baxter and Jack, an explanatory case study is used “[…] if you were seeking to answer a question that sought to explain the presumed causal links in real-life

42 Baxter and Jack, “Qualitative Case Study Methodology…”
43 Ibid, 544.
44 Baxter and Jack, “Qualitative Case Study Methodology…” 545.
interventions that are too complex for the survey or experimental strategies.⁴⁵ Though this thesis will seek to distance itself from the strict limits of causality, it is true that the number of factors in the case study are too complex and multifaceted to simply go from disinformation campaigns, to election meddling, and then to divisions in society. The inherent relationship between each of these components and steps are nuanced and convoluted at best, which is why this thesis will primarily seek to explain the phenomenon given the historical, socio-cultural context of the United States when necessary, and then analyze where there is room for improvement.

⁴⁵ Ibid, 547.
Primary Case Study: The United States

As the primary case study of this thesis, this chapter will explore both the context within which election meddling and disinformation campaigns were made to flourish, particularly citing the presidential elections of 2016, and the Midterm Elections of 2018 as key examples, in addition to the evolution of information institutions in the United States. The first section of this chapter will explore the impact social media had on the 2016 elections, including the Cambridge Analytica scandal, the nascent Fake News movement, and Russian troll factories and planted espionage experts. The second section will then discuss the evolution of information institutions in parallel with the U.S. understanding of strategic communication in practice. This chapter will conclude with a possible solution to the problem, a centralization of the institutions which monitor the information space in the United States in the form of a Ministry of Culture.


It is no secret that the 2016 Presidential Elections in the United States had a definite, clear effect both on how we conduct political campaigns, and on the information space itself. It was the culmination of social media conglomerates like Facebook and Twitter’s genuine lack of preparedness, and, some would argue, laziness, being brought into the light, an increasingly divided American population nearly ripping apart at the seams, and Russia’s hybrid toolkit making its debut in the West.

Just after the 2016 Presidential Elections in which Donald Trump, populist persona and business owner, defeated Hillary Clinton, by order of then sitting-duck President Obama, the Intelligence Community in the United States conducted an investigation into the then-alleged election meddling by the Russian Federation. In their January 2017 report, they concluded that not only were the elections meddled with, but that it “[...] represented a significant escalation in
directness, level of activity, and scope of effort compared to previous operations…”

The National Intelligence Council, the primary author of the report, even stated, “We assess Moscow will apply lessons learned from its campaign aimed at the US presidential election to future influence efforts in the United States and worldwide, including against US allies and their election processes. We assess the Russian intelligence services would have seen their election influence campaign as at least a qualified success because of their perceived ability to impact public discussion.” In other words, not only did the Kremlin amplify its efforts to influence U.S. elections in 2016, but also it is suspected that such efforts will—and have—continued, thus constituting a serious threat to national security. Though it was a multi-faceted approach comprised of social media algorithms, information warfare, and cyber espionage, social media took the forefront, due to a sincere lack of protection on the side of the United States. Though social media was only one tool used by the Kremlin in its attempts to meddle in the U.S. 2016 elections, it was arguably one of the more prevalent techniques, especially since there is no real mechanism with which to monitor or regulate what people post or propagate on their personal profiles. It is for this reason that this thesis will not address the issue of leaked emails or cyber hacks, especially since that is not explicitly related to strategic communication.

So how exactly did Russia ultimately influence the outcome of the 2016 elections? In early 2018, the European Parliament (EP) distributed a short report on the “Russian Troll Factory,” to go along in tandem with the previous 2017 report which attributed the meddling to the Russian Federation. This EP publication did not necessarily focus on the who, but on the how, entitled: “At a glance: Kremlin trolls in the US presidential election.” In the report, the result of years of research conducted by the Federal Bureau of Investigation (FBI) and the Central Intelligence Agency (CIA) culminated in the conclusion that over 50,000 bots who produced 2.1 million tweets, thousands of Facebook posts, and over forty hours of politicized

---

47 NIC, “Background to “Assessing Russian Activities and Intentions…”” Emphasis my own unless otherwise stated.
49 Ibid.
footage had attempted to influence the 2016 elections.\footnote{Russel, “Kremlin Trolls…” 1.} Beginning in March 2016, the Russian propaganda machine, made up of trolls, well-connected television and media producers, and Kremlin actors began promoting Donald Trump’s candidacy for President of the United States through social media platforms.\footnote{NIC, “Background to “Assessing Russian Activities and Intentions…””.} This was complemented by the consistent propagation of the narrative that Trump was being unfairly portrayed by the media outlets in the U.S., which unfortunately gave fodder to the infamous proclamation of “fake news” made by Trump later in his campaign, referring to nearly any negative information campaigns surrounding his candidacy.\footnote{In an interview, Trump claimed responsibility for popularizing the term “fake news.” See the full article here, Michael M. Grybaum, “Trump Discusses Claims of ‘Fake News,’ and Their Impact With New York Times Publisher,” New York Times, last modified February 1, 2019, https://www.nytimes.com/2019/02/01/business/media/donald-trump-interview-news-media.html.} These promotional narratives were further supplemented by trolls which tweeted and posted narratives which were aimed at both sides of the extremes in American politics: the far-right Tea Party conservatives, and the far-left millennial socialists. These 2.1 million previously mentioned tweets were either created by bots which would flood Twitter and Facebook’s newsfeed, and eventually, get retweeted by legitimate accounts, thus legitimizing the message, or Russian citizens would create so-called “shepherd accounts,” meaning they posed as American citizens’ accounts, which would then spread through “sheepdog” accounts, meaning Internet trolls, who would add their own content, and then the bots would propagate the message until it made it into the more legitimate news sphere.\footnote{Russel, “Kremlin Trolls…” 1.} The purpose of bots and in writing these tweets is sheer numbers and recognition, once they were picked up by a legitimate account and spread to that account’s network, the news was out and the goal was achieved. These tweets ranged on the political spectrum, but had the same goal in mind, one which harks back to The Kremlin Playbook’s suggestion: to target the inherent weaknesses in U.S. society, including its bipolar political system which draws harsh lines on the grounds of certain issues, at a time when its political transition was most vulnerable, the elections.

Tweets, however, are not enough to create divisions in society, they are only the start. After the seeds of discontent were planted, Russian workers located inside the United States created Facebook forums which spanned the political electorate, the most popular of which were “Heart of Texas,” “Being Patriotic,” and “Army of Jesus,” for the conservative right, and
“Blactivist,” “BlackMattersUS,” “LGBT United,” and “United Muslims of America,” for the liberal left. In creating these forums with over a combined million followers, it can be gathered that the Kremlin hoped to further liven discussions within the social media echo chambers, thus enhancing and incubating these activists’ views to a more radicalized point, that would stir up emotions and encourage them to spread their views and vote more vehemently. In creating the separate forums, they further deepened already existing divisions in the U.S. societal fabric. Importantly, these were already pre-existing points of contention, Russia did not create them, but simply benefited from the aftermath.

Once the forums were established and a group of supporters cemented, the protests and street riots began. In May 2016, an anti-Muslim rally was organized by the seemingly all-American, conservative group “Heart of Texas,” but was proven to actually have been organized by a few of the twelve Russians indicted by the Mueller report. This rally protested the Islamic Dawah Center in Houston, and rang not only of protests against the religion, but also of xenophobia, violent language, and threats. Though this site has since been deleted from Facebook, 249,000 people were counted among its followers, liking and sharing its posts on anti-Muslim rhetoric, as well as pin-pointing on a specific topic close to many Texans, Texan secession. Such argumentation focusing on a long-discussed, though generally discredited, topic puts on display the precision with which the Russian recipe for meddling within the United States was put together.

However, the single protest was not enough to increase the population’s ire. A counter-protest was also staged in front of the Dawah Center, and similarly to the “Heart of Texas” group, the “United Muslims of America” fan page was also created through Russian sourced media, resulting in sixty counter-protesters which naturally created more chaos and disagreement than the online forums. Other protests were staged, including numerous pro-Trump rallies

54 Russel, “Kremlin Trolls...” 1.
55 Ibid.
56 Tucker, “12 Russians indicted...”
58 Ibid.
organized by “Being Patriotic” with its 200,000 followers,⁶⁰ and by the BlackMattersUS group with a turn out between 5,000-10,000 protesters, according to one report.⁶¹ Once again, if we assume that Russia’s precise intention was to divide and create mistrust, stirring up discord on social media, with a smattering of disinformation, and then manifesting in staged protests was an effective tactic that reached over a million people.

The disinformation campaigns promoted ranged from a number of topics and reached a number of audiences. Aside from the consistent media coverage promoting Donald Trump both in the U.S. and internationally as the target of unfair American media smear campaigns, Russia Today (RT) and Sputnik, two notorious Russian media outlets, began themselves conducting what could be considered a smear campaign of Hillary Clinton. Not only were the Russians connected to the cyber attack on the Democratic National Committee (DNC), which negatively affected Clinton’s campaign, but they were also promoting Julian Assange, founder of Wikileaks, as a hero of free speech, and exposing corruption, for leaking Clinton’s emails.⁶² Aside from portraying Clinton in a negative light, and Trump in a positive light, the Kremlin also promoted more subtle, anti-Western and anti-democratic messaging. RT specifically is known for its strategic messaging connected to the elections and what it refers to as “the ruling class,” and even back in 2012, began a documentary dedicated to the Occupy Wall Street movement, declaring the U.S. political system corrupt and ruled by elites, with disinformation woven within the reportage.⁶³ According to the NIC report, such messaging has existed within the U.S. media space for nearly a decade, in order to sow discontent with the larger American democratic system,⁶⁴ and came to full fruition in 2016.

In addition, the Russian influence campaign in the 2016 elections was a multifaceted strategy, consisting of disinformation campaigns targeting salient issues within U.S. societal fabric, as well as cyber strategies and espionage that was made plausibly deniable due to the high

---


⁶² NIC, “Background to “Assessing Russian Activities and Intentions...””.

⁶³ Ibid.

⁶⁴ NIC, “Background to “Assessing Russian Activities and Intentions...””.
level of skill.\textsuperscript{65} Not only did the Kremlin appear to target think tanks, polities, and other political infrastructure believed to have a future influence on the campaign, but Russia also disclosed much of the information it gathered, all with the intent of undermining the democratic elections through “exposing” the corrupt underbelly of American democracy.\textsuperscript{66} Though the premise of this thesis is not focused specifically on the cyber aspects in depth, they are important to note to understand the extent of U.S. vulnerabilities, in addition to understanding the depth of the election meddling in its full context.

It is important to recognize that this thesis, nor the election meddling itself even, was or is about Donald Trump running for President.\textsuperscript{67} In fact, his style of speeches and rhetoric was merely an opportunity which was used to exploit further sentiment and mistrust in order to promote the Kremlin’s worldview over the democratic model. The divisions which were exploited by the external actors in the 2016 presidential elections are, unfortunately, themes which have divided the U.S. population for several decades, notably: guns, race, abortion, and immigration. Each of these themes has a deep-rooted, drawn-out rhetorical opus, however, this thesis will merely touch upon them briefly, then suggest further reading material should one wish to know more about the issue at hand.

The issue of gun control, or as its colloquially known, the second amendment debate, is certainly not new. However, as with most debatable issues, with the onset of social media, where each citizen has the opportunity to express their personal opinions with ease and speed, debates have since seemingly increased on the subject. In the Constitution of the United States, the 2nd Amendment in the Bill of Rights states, “A well regulated Militia, being necessary to the security of a free State, the right of the people to keep and bear Arms shall not be infringed.”\textsuperscript{68} The debate has stemmed over several factors, mostly concerning the intended scope of the amendment, for example, is the right to keep and bear arms only for those in this well-regulated militia? Or is it also intended for the layman? Out of this debate, many have extrapolated the amendment to protect their right to own many collector’s items, rifles, pistols, and others that

\textsuperscript{65} Ibid.
\textsuperscript{66} Ibid.
\textsuperscript{67} The author would like to note, therefore, that this thesis is in no way an indictment of the President of the United States, nor does it draw any conclusions as to his own wrong-doing necessarily, but does touch upon certain aspects under investigation and the entanglement with the Mueller report.

37
may not have an every day use, or could have been collected during a person’s military service. Nevertheless, others have found issue with the widened scope by some of the amendment, and linking the numerous school shootings and gun violence deaths across the country. According to Gun Violence Archive, 127 people have died in 2019 alone, with 376 injuries in the United States alone, and according to Vox, the U.S. is an outlier when it comes to gun violence in relation to crime. Even though gun homicides have declined in the past couple decades, the issue is salient to the U.S. population as they continue to see unnecessary deaths in their students and young population, stirring up calls to action. The main impediment to passing stricter legislation is notably the National Rifle Association (NRA), who, according to a CNN report, gave campaign donations ranging from $10,000 to more than $1 million to 684 members of Congress in 2018. With those kind of donations and other forms of lobbying, there is a clear explanation for the lack of concrete action, despite the numerous deaths. This issue, because it not only targets youth, but also innocents, is a very sensitive subject among U.S. Americans, and has been known to cause many emotions to run high. Therefore, it should not be surprising that it was one of the themes used in the election meddling and social media campaigns supported by the Kremlin. “Heart of Texas” notably mentioned second amendment rights “so [U.S. Americans] would forever be free from any tyranny,” which simply further divided people on the issue, practically as a reminder of the differences in opinion throughout the country on the divisive concept.

Race and ethnicity as an issue in American politics is also not new. In fact, it is an issue that can be traced nearly throughout the past two centuries. However, the issue of race has morphed and changed in the last decade especially, particularly with the election of Barack Obama in 2008, when many believed that showcased the importance of the “black vote” in

71 Ibid.
American politics, and more recently, with the onset of the Black Lives Matter (BLM) movement.\textsuperscript{74} The BLM movement began in 2013 after Trayvon Martin, a seventeen-year old teenager of color, was shot and killed, and the man accused of his murder was acquitted.\textsuperscript{75} The three founders, Alicia Garza, Patrisse Cullors, and Opal Tometi, all sought justice, and used their anger at the seeming continued prejudice against people of color in the United States. Since then, the Black Lives Matter movement has hosted countless rallies, protesting against police brutality, particularly perpetrated against the Black community and other people of color, and the need for a change in the overall socio-economic system quietly prejudiced against them. Race in the United States is an issue with deep roots in history, however, and it cannot be employed without heightened emotions and tension. Given the larger context of the Civil War, largely believed to have been fought over race,\textsuperscript{76} then the continued segregation and degradation of people of color in the Jim Crow era, and finally through the Civil Rights Movement with Martin Luther King Jr. and Malcolm X, the contention of race and prejudice causes many in the U.S., and around the world, to bristle at the thought of racism or xenophobia, creating tensions and at times, defensive behavior resulting in greater divides. Race relations are notoriously tense in the United States, and it was clear that the election meddling used it as a weak point, at which it aimed disinformation campaigns and various social media tactics, particularly through forums and protests.

Abortion is an issue that concerns women’s rights and the women’s movement, another divisive issue in the United States. The question of “pro-choice” or “pro-life,” has been asked in the U.S. for several decades, and not only portends to the rights of female bodily autonomy, but also extends to a question of religious morality. The landmark case of Roe v. Wade in 1973 marks the center of the issue, in which the U.S. Supreme Court ruled in essence that abortions were legal up until the point that the fetus was not viable outside the womb, in other words, during the first trimester, based on a woman’s right to privacy enshrined in the fourteenth

\textsuperscript{74} For more information on the black vote, see Katherine Tate, “From Protest to Politics: The New Black Voters in American Elections,” Political Science Quarterly 109, no. 1 (May 1994).


\textsuperscript{76} However, there is a historical narrative, particularly taught in the South, that denies the Civil War’s relation to race, and teaches that war broke out in 1861 primarily due to the issue of Secession of the Confederate States.
amendment.\textsuperscript{77} In other words, a state or industry could not refuse a woman an abortion in the first trimester due to her right to privacy and control over her own body. Nevertheless, in 2019 alone, more states have been restricting access to abortions, most recently resulting in the State of Georgia’s notorious “fetal heartbeat” law, restricting access to abortion after only six weeks of pregnancy, the time when a doctor usually can detect a fetal heartbeat.\textsuperscript{78} Though the law may still be challenged in the state Supreme Court like the others of 2019,\textsuperscript{79} its proponents claim to protect the lives of the children that otherwise would be killed due to previous, irresponsibly poor choices on the part of the parents. Much of these beliefs are upheld by a religious, moral standard, and often incite strong feelings on both sides of the debate. When signing the bill into law, Georgia Governor Brian Kemp stated, 

\begin{quote}
[...] we protect the \textit{innocent}, we champion the \textit{vulnerable} [...] The ‘Life Act’ is very simple, but also very powerful, a declaration that all life has value, that \textit{all life matters}, and that all life is worthy of protection [...] Our job is to do what is \textit{right}, not what is easy. Through the ‘Life Act,’ we will allow all babies to grow up and realize their full \textit{God-given potential}.\textsuperscript{80}
\end{quote}

In this quote, we can also see the connections to the previous theme of race, by stating that “all lives matter” instead of black lives matter, in addition to drawing upon moral standing. By reiterating the “right” path, protecting the innocent, and helping children grow up to realize their “God-given” potential, the question of abortion goes beyond privacy, and reaches into the religious Christianity of much of the United States, which stirs up strong emotions and divisions in the society.

The final theme, immigration, while also not considerably new, was perhaps the strongest rhetorical argument used in the 2016 presidential campaigns, particularly in the case of now President Donald Trump’s stance on building a wall across the U.S.-Mexico border. Throughout


\textsuperscript{79} Six states have currently attempted to pass so-called ‘fetal heartbeat’ bills in the United States in 2019: Ohio, Mississippi, Kentucky, Iowa, North Dakota, and Georgia. For more information, see Madeleine Aggeler, “The Terrifying Rise of the 6-Week Abortion Ban,” The Cut, last modified May 10, 2019, \url{https://www.thecut.com/2019/05/which-states-have-passed-six-week-abortion-bans.html}.

\textsuperscript{80} Maze and Blinder, “Georgia Governor Signs…” Emphasis my own.
the campaign, immigration was one of the most talked-about topics. According to the Center for Immigration Studies, immigration played an “unusually prominent role” in the presidential campaigns, and, according to their research, “polarized opinion by partisan identity more than at any other time in contemporary history.” Immigration is not simply an issue concerning race or even religion, though in a post-9/11 world it certainly is a factor, but it is also an indication of the population’s fear of a perceived lack of job growth, and connects to other economic woes of U.S. society.

Each of the previously mentioned four issues—guns, race, abortion, and immigration—cut across class and racial divisions, and across state lines, making them the most salient issues for the majority of Americans, aside from perhaps select issues of the economy. Each of the topics are extremely personalized in U.S. politics for a number of reasons, and usually involve high emotions because of identity politics, moral values, and in particular, how they affect the lives of children. Unlike guns, abortion, and immigration, race is less of an issue in political debates themselves, though it still often determines how populations in certain states vote, and is an age-old tension in the U.S. societal fabric. In a Pew Research Center poll, all four of these issues were considered to be “very important” to their vote in 2016 by 50% or higher on average of the registered voting population. Each of these themes was also subject to various disinformation schemes, which puts into practice what was talked about in the previous chapter regarding disinformation and its connection to election meddling. All of this furthered the same goal, to cause mistrust and chaotic sentiment among the people which resulted in the election of an official more believed to be more agreeable to the Kremlin’s cause. U.S. societal vulnerabilities and divisions are perhaps most present in these four concepts, and are thus the main issues to be focused on when attempting to address the root causes of, and combat, the threat.

Unlike the European Union, which established a governmental, overarching body aimed at keeping track of the disinformation campaigns present in the European media space, the United States took a notably different approach in response to the 2016 elections. After reports of

---

the foreign meddling were released, lawmakers and citizens alike turned to the social media conglomerates Facebook and Twitter, to better understand how this could have happened without the companies knowing, or really seeming to do anything to impede such a phenomenon. Then, in March of 2018, a trio of newspapers, consisting of the New York Times, the Observer, and the Guardian, came forward with a cache of documents which suggested that Facebook had mined voter’s personal data and sold it to a firm in London called Cambridge Analytica. The firm was then discovered to have been connected to Steve Bannon, one of then presidential candidate Trump’s political aides, with the purpose of profiling potential voters in order to better promote their campaign to win votes. Cambridge Analytica had developed a personality quiz, reaching and mining the data of over 80 million Facebook users, and based on their answers to the questions and social media algorithms, the cross-comparative study was meant to showcase who the social media user would potentially vote for in the upcoming elections. Though trying to discern the sway or political leanings of swaths of the population is nothing new in the U.S. election context, the data mining issue became uncomfortable for people who felt that their right to privacy had been violated, and resulted in the special hearing of Mark Zuckerberg, owner and CEO of Facebook. Zuckerberg, when asked about his company’s role in the scandal, apologized, though claimed that Facebook believed Cambridge Analytica to have only used the data of users which permitted it, and that once the contract ended they no longer had access to it. The apology was noted, but perhaps not well-received by the majority of the population. Since the elections, Facebook has changed its privacy policy and its tactics regarding disinformation, in order to prevent a similar data mining scandal, and further election meddling. However, social media conglomerates such as Facebook have been the primary target of the government’s

84 Ibid.
scrutiny in combatting disinformation campaigns and the propagation of fake news. The U.S. government therefore has visibly cracked down on social media outlets for their role in the threat, which naturally, does address at least part of the problem. However, the larger divisions within the U.S. societal fabric is not going to be addressed by forcing Facebook to take down pages propped up by Russian bots. Strategic communication is needed to address the root causes and the targets of Russian election meddling.

To everyone’s relief, in 2018, the Department of Justice (DoJ) and the Department of Homeland Security (DHS) found foreign meddling to have had “no material impact” on the outcome of the midterm elections, according to a joint report they shared with the President.\textsuperscript{88} This showcases not only a slight shift in awareness of the threat, nevertheless, the report remains classified, and while experts assured that the integrity of the elections were not compromised, they did not indicate that social media, propaganda, or even disinformation did not ultimately play some kind of role. In so doing, the security nexus of elections remains firmly within the technological sphere, and not rooted within the information and media sphere, which continues to leave the United States as vulnerable to societal divisions, as it was almost four years ago.

2. Background on U.S. Information Institutions and the Evolution of Strategic Communication

Though we have defined what strategic communication means in the academic world—and for this thesis—strategic communication is not just an idea or a concept, it is factually embodied in information institutions of the government representing a particular state, and if its utilization is to be argued for combatting disinformation and election meddling, then it follows that further investigation into strategic communication and its impact is imperative. Strategic communication is performed and shaped by the organizations which utilize it to their own advantage. It therefore goes beyond merely what it means, but also how it has been used. Its use should be outlined when explaining what more can be done, and this section will show how

strategic communication—or better yet, the lack thereof—has operated in the context of the United States, specifically in the U.S. Government.

As Glenn Andrew Crowther explains in his article “100 Years of Information Competition” (2019), since the Founding Fathers, the United States has been subject to, yet at the same time wary of, information operations designed to influence the population.\(^8^9\) Like most states, the U.S. Government used information operations during wartime, apparatuses which quickly dissipated as soon as peace settled in so as not to continue promoting a “pro-war” agenda when there was no war to fight, or to render the agencies illegitimate should they pop up again. However, with the ideological Cold War, the United States needed a response to the information operations and pro-Soviet propaganda of the time, even if it was not at risk of physical war. In 1948, President Truman designated two avenues of information operations: covert, which were enshrined—and arguably still are—within the Central Intelligence Agency (CIA); and overt, within the Information and Educational Exchange Act (IEEA), popularly known as the Smith-Mundt Act.\(^9^0\) The Smith-Mundt Act is known for being the main legislation banning external propaganda in the United States, but it also is “to enable the Government of the United States to promote a better understanding of the United States in other countries, and to increase mutual understanding between the people of the United States and the people of other countries.”\(^9^1\) Important to note in this legislation, is the dual purpose enshrined in its writing; not only does it promote information to foreign countries about the United States, its regulations and governmental system, but it also promotes educational exchanges between people of the United States and other foreign countries. Strategic communication enshrined within the Smith-Mundt Act is therefore primarily focused outward, in what the author will further refer to as internationally proactive strategic communication. As was previously mentioned, internationally proactive stratcom is an information operation that is primarily focused outward, and is a form of foreign policy designed to engage with like-minded allies. Soon after the IEEA, the U.S. Advisory Commission on Public Diplomacy (ACPD) went on to be created within the U.S.

---


Department of State, and the work it produces is often now referred to in the United States as public diplomacy.\(^{92}\)

The United States during the Cold War did include strategic communication in some form in their national security paradigm, though such efforts seemed to end after the Soviet Union gradually collapsed in 1991. Information warfare was even named in the National Security Council’s (NSC) report in 1950, and was incorporated in two points:

- Development of programs designed to build and maintain confidence among other peoples in our strength and resolution to wage overt psychological warfare calculated to encourage mass defections from Soviet allegiance and to frustrate the Kremlin design in other ways; and, intensification of affirmative and timely measures and operations by covert means in the fields of economic warfare and political and psychological warfare with a view to fomenting and supporting unrest and revolt in selected strategic satellite countries.\(^{93}\)

Within this report, there are two main issues to focus on. The first, is what is being done, and the second is the purpose for which the United States was waging information warfare. The two policies as stated in the above quote are to maintain the population’s (both foreign and domestic) confidence in the U.S. ability to wage information warfare, and the second, is to enact timely covert operations. Both of these points were to assist in both encouraging defection from the Soviet regimes, and supporting unrest and revolt, which therefore constitutes the notion of warfare. By aiming to inspire revolt and resistance in the satellite states of the USSR, and encourage defection by Soviet elite and those in the Kremlin, the U.S. was targeting both those within and without the larger system. In the chapter discussing the case of election meddling in the United States, we will see how this same sort of technique has adapted to the times of technology.

The significance of the subsequent absorption of information warfare in the national security paradigm should not be underestimated. As the Soviet Union was seen as an adversary of the United States, this gave the security community the justification, and then swiftly the

---


\(^{93}\) Glenn Andrew Crowther, “100 Years…” 108. Emphasis my own unless otherwise stated.
means through its consequent securitization\textsuperscript{94} vis à vis the National Security Council’s report, to enact a public diplomacy campaign through the United States Information Agency (USIA).\textsuperscript{95} Particularly important to note, however, is that all of the forms of information warfare noted in the NSC’s 1950 report being waged fall under public diplomacy, which is inherently targeted towards the foreign world, which creates the largest distinction between strategic communication and PD.

In an interview with a source within the U.S. Department of State, public diplomacy was described as “outreach to foreign audiences” through people to people connections, rather than through governments and heads of state.\textsuperscript{96} Such outreach is conducted in three ways, through civil society via non-governmental organizations; public relations, events, and affairs; and the media, all of which inherently roots it firmly in foreign policy. Therefore, public diplomacy and strategic communication are not to be used synonymously, since the former can only be used in an external context, while the latter can be used both with foreign and domestic audiences, as this thesis argues. Furthermore, stratcom is simply one of the instruments upon which PD is based.

As previously mentioned, the Smith-Mundt Act, considered the founding document of PD and stratcom, promoted not only positive messaging and communication, but also educational and cultural exchanges, which now fall under the larger umbrella of public diplomacy. However, Smith-Mundt in writing the rules of the game also created the biggest obstacle to effective strategic communication: the public diplomacy being conducted abroad cannot correlate to, nor correspond with, strategic communication or public relations within the United States in the domestic sphere. Though public diplomacy is founded on the interests of the home government of the time, that is the extent of its relationship with the domestic sphere. Such red tape, though it is to protect the domestic media from being too canonized and to protect First Amendment freedoms, leads to institutional confusion, and lack of a clear mandate. According to the State Department’s anonymous source, the State Department handles public diplomacy abroad, while the Department of Justice (DOJ) and the Federal Bureau of Investigation (FBI)

\textsuperscript{94} For the sake of clarity, this thesis follows the traditional teachings of the Copenhagen School, and their belief that securitization is a speech-act articulating a certain threat which is rooted firmly within linguistic rules of speech and is generally accepted by an audience.

\textsuperscript{95} This Agency is no longer being used, as it closed in 1999 after it was subsumed into the Department of State into the Bureau of Educational and Cultural Affairs (ECA).

\textsuperscript{96} Source to remain anonymous. Interview with the author. April 3, 2019, Washington DC, USA.
monitor public relations and media campaigns within the United States. There is therefore no single body which handles strategic communications domestically.

There are several reasons for this, which will be elaborated upon further in the next section, but it should first be made clear that such a lack of centralization is, according to the author, one of the major causes of the U.S. vulnerability to disinformation campaigns and election meddling. Without a clear centralized point, each entity which is designed to combat disinformation, including the media literacy non-governmental organizations, civil society platforms, and other activist firms, do not have a place where they can strategize together, or develop coherent, cooperative mechanisms with which to counteract such negative narratives. Without a coherent strategy or messaging system, it creates further chaos in the information sphere, which overwhelms the already apathetic population, furthering the negative spiral of mistrust in media and journalism, and deepens the divide between the conservative right, and the liberal left.


But if it is so essential, why is there no such body? The United States since its inception, as mentioned before, has been a state built upon certain freedoms and certain expectations of the population. Enshrined within its founding document, the freedom of press, protest, religion, and speech are arguably the most famous rights which begin the Bill of Rights of twenty-seven amendments. Written in protest against British Imperial rule in 1791, the Bill of Rights encompassed the greatest grievances as viewed by the former colonies, including having an overarching power which controlled all aspects of life, including taxes, popular opinion, and other policies, without any say from the people.\(^7\) It is no secret that the United States has since become a country based on the founding principles of “We the People” before the administration of the time. Such thinking can therefore be reflected in the belief in the freedom of the press, and

Therefore, the wariness in controlling, or centralizing the media under one body who could come to control the U.S. general response to negative or unflattering narratives.

Such a feeling has persisted throughout American history, but arguably became amplified during the Cold War. As the narrative wheel began to spin, depicting capitalism versus communism, freedom versus totalitarianism, the United States versus the Soviet Union, the feeling of anti-centralization sharpened, in spite of a spike in bureaucratic institutions and expansion of government agencies due to the securitization of the ideological war being waged. While the state apparatus grew enormously after World War II\(^8\) to accommodate the evolving security environment and new technological wave, the people’s belief within the United States in their personal freedoms only grew, and a fear—and in some cases, hatred—for totalitarianism surged. Such disdain does not simply go away, and in fact, when compounded with a historical narrative of a nation founded by throwing away the shackles of colonialism, and promoting the rights of the layman above those in power, you get a strong resistance to any large, overbearing ministry which monitors information flow. When compounded with the largely diverse national character of the United States through its generations of immigrants and intermingling of cultures and races, having one voice that overpowers all others is simply infeasible. This characteristic mistrust of one voice is one of the persistent reasons, the author maintains, that a Ministry of Culture, which could act as some sort of monitor over information flow, has thus far not been created.

However, as previously mentioned, this absence of a central body in fact enlarges the problem, in addition to being a product of the larger national sentiment. Such fear of centralization, though understandable in the 1940s, is simply no longer viable in the age of technology: an increasingly interconnected and disintermediated\(^9\) world. As the world wide web has no borders, it is difficult to track and control, especially as social media sites increase the number of user-created content and brand ambassadors on their sites. Therefore, in order to best regulate—or at least monitor—possibly malignant content on the Internet, a centralized body would be the best way to do so.

---


\(^9\) Professor Alan Tidwell of Georgetown coined the term *disintermediated* world to describe the limitless bounds of the Internet, and the clear absence of gatekeepers in the world of social media.
With the sheer volume of information out there, how would a Ministry of Culture assist in its classification or monitoring? An exemplary model which would make the most sense for the U.S. context can be found in its political campaigns. For every campaign, there is a communications team—much like those in a corporation or business—of speech-writers, analysts, and those who monitor the press and oversee communication being published by the campaign. These teams however, not only watch their output, but also observe what is being said about their candidate, so they can then come up with an effective counter-narrative in response to negative press. According to corporate strategy, such responses would fall under the umbrella of strategic communication, which is what was previously noted in the Theories and Methods chapter of this thesis. Candidates which have an effective stratcom team typically run the most successful campaigns, especially in the age of the internet and social media, because it can reach its audience much more efficiently, effectively, and expeditiously. So, if the individuals running for the U.S. Government positions have such effective stratcom, what happens once they are in office? Why is it that the U.S. Government itself does not have an effective strategy for communicating with its population? A Ministry of Culture could bridge such a gap between the war rooms of political campaigns which effectively respond to negative press—which at times could be considered as disinformation campaigns depending on the content—and after they are elected and in office. In other words, the U.S. Government needs its own “war room” which could effectively respond to untruthful, negative campaigns on a large scale, in order to reignite public trust in the U.S. Federal Government.

Democracies appear to have fallen under the illusion that loyalty to the state is a given, but it has to be earned. In the age when information is at everyone’s fingertips, including falsified information utilized for personal gain, respect and loyalty to one’s state is not automatic, and truthfully, never has been. Of course, loyalty or trust in the state allows room for disagreements, in fact, debate is often stated as being the medicine for keeping democracies healthy. Nevertheless, we cannot stand idly back, and expect the citizenry’s allegiance to the state to kick in in a time of need. It is not enough to simply negate the negative narratives of disinformation, to fact check, and have the truthful headlines run at the bottom of the screen

during a debate, as was done in 2016, or to encourage sources like NPR to fact check everything
candidates say and keep a running tab.\textsuperscript{101} If fact-checking were enough, the European Union
External Action Service’s (EEAS) East StratCom Task Force would not only be more successful,
but also the bulwark against disinformation spreading in the EU’s borders. Its webpage of
EUvsDisinfo, though helpful if one knows where to find it, simply results in a litany of facts and
rings of “he said, she said.”\textsuperscript{102} In fact, in an interview with the author, a State Department
employee maintained that the EU’s East StratCom Task Force was not meant for the public at
all, but really to be used as a tool by Europe’s politicians when drafting legislation.\textsuperscript{103} Though
admirable, and certainly important, fact checking the disinformation campaigns, and keeping
track of every false thing said in European media has not changed the number of campaigns in
the continent, nor has it seemed to have had any effect on their salience. NPR in the context of
the United States, unfortunately, runs parallel to the Task Force, and has had no sincere impact
on the number, nor the ramifications of disinformation campaigns.

There are, according to the author, two primary reasons for this. First, those who come in
contact with disinformation in the United States, which in the 2016 elections were not that many,
will not necessarily be the same people who fact-check their sources or the stories they hear on
the news. The people who utilize these sites, besides lawmakers, would be people concerned
with the integrity and validity of the information they promote, which does not necessarily
overlap with a citizen simply idly scrolling through social media, and reading the top lines of
articles. Second, and perhaps more importantly, fact-checking alone is not enough to combat
disinformation campaigns because it is akin to sticking a bandaid on an old wound and expecting
it to heal entirely, it cannot. When addressing threats, security experts must look at the outcome,
and the root causes, and attempt to address both in a two-pronged strategy, much like what has
been done to counteract terrorism, crime, and other threats we face.

So what can and should be done? Realistically, the previously mentioned idea of a
Ministry, or perhaps considering the context, a \textit{Department}, of Culture for the United States
would face many obstacles in its establishment, as was noted. Not only is there no historical
basis for such a body, but also there would be many who fear its scope or what it could come to

\textsuperscript{102} See EUvsDisinfo, last accessed May 10, 2019, https://euvsdisinfo.eu/.
\textsuperscript{103} Interview with the author, April 3, 2019, Washington DC, USA.
represent. Nevertheless, a single body should be established to gather information on what is being said, both within and without about the United States, and to monitor the disinformation. However, this body should not necessarily address the root causes, since its legitimacy in the matter would most likely be questioned by an already skeptical American public, but simply attempt to accumulate the ways to negate the negative narratives to avoid confusion. Instead, the root causes should be addressed primarily through education. Media literacy courses have already been established in some schools across the country, and students already learn how to discern a “good” source from a “bad” source when they begin writing short essays so as to avoid plagiarism. But, these courses do not address disinformation campaigns, or at least, not substantially, and they definitely do not address how social media works.

Therefore, the author posits that social media literacy courses be established in every middle school and high school across the United States, in order to ensure that the next generation of American citizens not only grow up understanding the world of information, but also become cognizant of the technological, social world they will inevitably grow up in. These courses, preferably taught once in middle school for thirteen to fourteen year olds, and once in high school for sixteen to seventeen year olds, should cover not only how to recognize a “good” source from a “bad” source for a school paper, but also in the media, to understand that every channel they or their parents listen to will have a slight slant. Such a slant is not inherently bad, so long as it is recognized by the viewers and not taken as unadulterated, immovable fact. Furthermore, these courses should also include a basic overview of social media algorithms. Though lacking in technicality, a basic understanding of social media is clearly needed to increase the U.S. society’s awareness of how election meddling is possible in the information sphere, and how sites like Facebook and Twitter are meant to show you want they think you want to see. Students should receive an overview of how echo chambers work, how the more you click or “like” posts from a certain page, the more often they will show up in the newsfeed due to cookies and other data mining methods on the internet. While sounding overly technical, these lessons could be made quite simple to understand for students, particularly through interactive exercises which split people into groups with slightly different information, like echo chambers, and then being made to go around and explain their story to others from different echo chambers.

---

Once students recognize that computers and technical algorithms try to categorize human beings into simplified characterizations, then the next generation may begin to understand the nuances of the information sphere, and be more well-versed in media literacy, than we are today.

Of course, such courses do not address the problem at hand of election meddling, which is why these must be conducted in tandem with efforts on the part of the government to utilize domestic, proactive strategic communication in order to effectively reignite a sense of cohesion among the U.S. citizenry. It is not enough to only address the root misunderstandings by teaching the next generation of voters, just as it is not enough to simply have a fact-checking body to negate negative narratives. It is certainly a long-term process to try to bring together both sides of the aisle, and it certainly will not be an easy feat. However, strategic communication is needed in order to bridge the gap between the widening divisions in U.S. society, especially on issues previously highlighted, such as guns, race, abortion, and immigration. If the government cannot promote a common message due to its inherently limited political ideologies and interests, then there must be a body which attempts to represent the interests of the American people at large. Trust and faith in the U.S. government must be reestablished in order to encourage societal resilience and prevent further possibility of election meddling, which is why strategic communication is the answer. Both education of the next generation, and fact-checking of current narratives, in addition to the promotion of a common thread of understanding have to be done in tandem in order to promote the overall goal of the U.S. government: to protect the freedom and integrity of the democratic process, and ensure “liberty and justice for all.”
Conclusion

In the Office of the Director of National Intelligence 2017 report, the U.S. Intelligence Community notes that the Kremlin’s model of election meddling is here to stay, and is a long-standing trend which we will have to continue to face and counteract for the foreseeable future.\textsuperscript{105} If that is indeed the case, which is quite reasonable to assume, then combating information warfare in the United States is not to be treated as a simple past-time, something that will happen and be promoted by a select group of media literacy experts and activists, and then simply gather dust on the top shelf. This is a strategy which needs to not only be taken seriously, but also actively employed in order to prepare the U.S. voting citizenry for the upcoming elections in 2020, and beyond. In recognizing that information warfare is something which will continue into the next few decades, especially as technology and social media continue to expand and improve, the issue of disinformation, and utilization of strategic communication is not to be taken lightly.

This thesis has walked through the limiting definitions of strategic communication, and attempted to highlight the shortcomings of current academic discussion surrounding it. By binding it to a concept which is only used outside the United States and not within, the U.S. restricts its ability to handle disinformation campaigns on its own soil. By not hosting a singular body under which an umbrella of strategic communication could be enforced, the U.S. lacks a coherent strategy to address the threat domestically, and remains vulnerable to the information warfare tactics of the Kremlin. Such tactics of disinformation and election meddling were discussed in the previous chapter, highlighting that the U.S. vulnerabilities to such tactics lie in its increasingly wide divisions, especially on issues which illicit emotional responses because of their rhetorical connection to morality, religion, or the lives of children. In addressing such vulnerabilities, the U.S. needs to have a body, likely a new Department or Ministry, which not only promotes a bipartisan stance, but also continues to encourage societal resilience to disinformation through fact-checking, and raising awareness of the dangers of falsified information and election meddling. However, in order to increase the efficacy of counteracting the information warfare threat, there must also be continued education of the next generation of voters, not only on the qualities of good or bad media sources, but also on a basic understanding

\textsuperscript{105} NIC, “Background to “Assessing Russian Activities and Intentions…””.
of how social media works to categorize and pigeon-hole people based on their “like” patterns and clicks on certain kinds of articles. Such a strategy must be a continued effort, in order to combat this growing threat to the domestic security of the United States, and the integrity of its future elections.

Russia as a revisionist actor in the 21st century has been arguably largely ignored by the West, to the detriment of both our international security, and domestic sovereignty. The Kremlin was not seen as an actor which could take on Western societies and democracies head-on, and therefore was not recognized for its opaque, malign, opportunistic tactics utilizing growing technology and the interconnectedness of our world. Russia does not underestimate the power of winning hearts and minds, and continues to cater its strategy to the unique situation of each country it attempts to meddle in—our counter-strategy must do the same. Each Western government must think beyond the problems at hand, and consider the weaknesses that the Kremlin is simply taking advantage of, and capitalizing on, rather than believing them to be vulnerabilities which Russia creates. The United States in particular needs to address its own societal vulnerabilities, in addition to what it does abroad with Public Diplomacy, and the Global Engagement Center. The threat is not merely with its allies, but also clearly on the home-front.

In 1992 Francis Fukuyama notoriously declared the “End of History,” and lamented the loss of the “good old days” of dual hegemony, and purported that the future was multilateral and seemingly dull because there would be no ideological war between the United States and the Soviet Union.\(^{106}\) It is clear that he was further from the truth than he realized, but the West has seemingly continued to underestimate what the former Soviet Union, now primarily the Russian Federation, is willing to do to regain its place in the world as a global power, one which continues to contest the democratic, liberal world order proposed by the United States and the West. Though information warfare is now recognized in most strategic documents, the Western world, and the United States in particular, must do more than simply include it in its long security document, but take action, one which addresses the threat of disinformation, and looks to its own vulnerabilities, and instill societal resilience, and trust in the democratic system.

---

Bibliography:


Interview with the author. April 3, 2019. Washington DC, USA.


Thorson, Kjiersten. “Strategic communication.” Communication (September, 2013).


