THE PENNSYLVANIA STATE UNIVERSITY
SCHREYER HONORS COLLEGE

THE COLLEGE OF INFORMATION SCIENCES AND TECHNOLOGY

MEDIA ENABLED INFORMATION OPERATIONS: A FRAMEWORK FOR THE 2020 U.S. ELECTION

CALVIN D. MENDE
SPRING 2020

A thesis
submitted in partial fulfillment
of the requirements
for a baccalaureate degree
in Security and Risk Analysis
with honors in Security and Risk Analysis

Reviewed and approved* by the following:

Colonel Jacob Graham
Professor of Practice of Information Sciences and Technology
Thesis Supervisor

Donald Shemanski
Professor of Practice of Information Sciences and Technology
Honors Adviser

* Electronic approvals are on file.

ABSTRACT

During the 2016 presidential election, Russia launched an information operation on a scale never before seen. The Russia-based Internet Research agency was able to spread disinformation and sow political discord among U.S. citizens through the use of social media. By creating a deception narrative, Russia sought to undermine Western democratic principles. The U.S. has made efforts to respond to Russian interference. However, with the 2020 election approaching, Russia will be seeking to influence citizens for a desired effect. This report will complete the following: define and analyze information operations from the scope of the United States and Russia, define the elements of deception, examine the biases that make individuals susceptible to deception, identify social media's role in disinformation, study the effects and implications of Russia's interference in 2016 election, and provide a theoretical framework for the potential intentions and actions of Russia in the 2020 U.S. presidential election.

TABLE OF CONTENTS

LIST OF TABLES

ACKNOWLEDGEMENTS

Foremost, I would like to express sincere gratitude to my thesis supervisor, Col. Jake Graham. His mentorship and guidance throughout this process was invaluable. I would also like to thank my honors adviser, Don Shemanski. He provided encouragement and assistance that helped me reach my academic goals. I need to thank the Schreyer Honors College for providing countless opportunities to better myself. Finally, I would like to thank my parents, Doug and Crystal Mende, who served as a support system through times of stress and uncertainty during my career at Penn State.

Chapter 1

Introduction

At dawn of our nation, the founding fathers recognized the danger of allowing foreign nations to interfere in U.S. elections. Efforts were made to guard against foreign interference by requiring the president to be a natural born citizen and creating the Emoluments Clause that prohibited any government officer from accepting a title or gift from a foreign government (Elving, 2019). The framers of nation understood the dangers of allowing the democratic process to be affected by foreign entities. The fears of the founding fathers were realized during the U.S. 2016 presidential election. Russia was able to interfere on a scale never before seen due to social media enabled information operations.

Information operations have existed for centuries. As technology advances, the strategies to employ information operations become more intricate. USSR and Russian influence operations rely heavily on foundations of deception. These principles have been present in conflicts throughout Russian history and are highlighted during the Cold War. Deception operations consist of identifiable elements present in all cases. Among these elements are biases that allow an individual to become susceptible to deception.

Russia's interference in the 2016 election featured a dominant use of social media to shape public perceptions. Through the Internet Research Agency proxy, Russia was able to spawn an unprecedented amount of false accounts; each with the ability to spread vast quantities of disinformation. With the 2020 U.S. presidential elections approaching, it is essential to understand the intentions, goals, and potential actions of Russia's information operations.

Chapter 2

Information Operations

Introduction

Information warfare is not a new phenomenon and has been in existence well before the term was coined in the military lexicon. The Chinese general and military theorist Sun Tzu believed all warfare is deception, and established the power that controlling information and disinformation can have (Komar, 1995). The progression of information warfare has paralleled the advances of technology. The invention of the radio transmitter gave the enemy the opportunity intercept, monitor, and spoof electronic communications. The use, or rather the reliance, of technology enables new domains that the enemy can target. Without proper identification and fortification these domains can threaten the United States on a strategic level. The involvement of computers in aspects of everyday life has allowed the cyber domain to become a target ripe for adversaries.

United States Definition and Employment

In 1998, the United States gave information operations (IO) a broad definition of actions taken to affect adversary information and information systems while defending one's own information and information systems (Shelton, 1998). In 2012, this definition was updated to describe the increasing growth of communication technology and free flow of data around the world (Scaparrotti, 2012). The modern United States characterization designates three sections of

the information environment: the information dimension, the physical dimension, and the cognitive dimension (Scaparrotti, 2012). The information dimension incorporates where and how information is collected, processed, stored, and disseminated; directly affecting the content and flow of information (Scaparrotti, 2012). The physical dimension contains command and control systems, decision makers, and supporting infrastructure; components within this dimension all fall within the real world (Scaparrotti, 2012). The cognitive dimension involves the minds of those who transmit, respond, or act on information; considered the most important of the dimensions (Scaparrotti, 2012). These dimensions are continually interacting within the information environment and shortfalls in one dimension can have impacts on others.

As an element of statecraft, information operations are available during crisis and peace. Economic sanctions are a tactic of foreign policy that have been viewed as slow moving and direct, but IO can occur quickly and cause severe damage with a low level of violence (Barnett, 1998). Given the results IO can potentially create, the United States has placed an added significance on both defending against IO and expanding our own capabilities (Barnett, 1998). There exists a potential for IO to prevent conflicts during peacetime and respond effectively during a crisis. Despite the peacetime capabilities, the U.S. has reserved information operations mainly during times of hostilities.

The Department of Defense recognizes five core capabilities of information operations: psychological operations, military deception, operations security, computer network operations, and electronic warfare (Wilson, 2007). Psychological operations involve the use of information as propaganda to influence emotions, motives, and behavior of foreign governments, groups, and individuals. Military deception is comprised of actions taken to deliberately mislead adversaries, with a focus on disinformation. Operation security utilizes the process of identifying critical

information and analyzing friendly action toward military and other operations. Computer network operations consist of offensive and defensive actions taken in cyberspace. Electronic warfare is defined as any action attempting to control the electromagnetic spectrum or to attack an enemy, examples include jamming or disabling enemy global positioning systems or radio communications. IO has a large appeal to countries who could not otherwise compete with the United States within the traditional symmetric warfare environment. The cyber-terrain is full of constant attacks on U.S. infrastructure due to the low cost and anonymity the Internet provides. Terrorists and some non-state actors have utilized the Internet and information technology to accomplish a wide variety of tasks from disseminating messages to detonating improvised explosive devices. In the past, these would not have been possible without extensive resources, but have become commonplace, enabled through cyberspace. Each of these attacks raise an interesting concern surrounding U.S. retaliation. Through the Law of Armed Conflict, the U.S. response will be scaled in proportion to the attack and distinctions will be made to combatants and civilians. This definition is highly reliant on the scope of traditional kinetic warfare, and does not directly apply to the capabilities of a cyber-attack. This highlights the slow process the U.S. legal system has been forced to employ in adapting policies. As we enter a new age of information warfare, the legal atmosphere is already behind the capabilities of U.S. adversaries.

In warfare, there is a concept known as amplifiers. These are factors that shape the battlefield in a non-linear manner; that is, they not only accelerate previous trends, but also redefine war. In World War I, the application of chemistry and chemical engineering changed how war was fought. In World War II, the destructive discoveries of physics shaped the battleground, ranging from the use of the atom bomb to wireless and radar capabilities. Throughout the Cold War, information researchers exploited intelligence and knowledge of the

enemy and allowed the U.S. to defeat the Soviet Union with a relatively small loss of life. It has been suggested that the next emerging amplifier will be influenced by human beings themselves rather than technology or bureaucracy (Scales, 2009). Highlighted by some modern "psycho-cultural" wars, it may no longer be about capturing and maintaining an area, but rather capturing the perceptions of the target population. This idea becomes further reinforced by the shape battlefields are more commonly taking. Rather than a set of contested geographic zones vying for control, modern battlefields are nebulous, dispersed, and ill-defined. In order to keep up with the focus on psycho-cultural aspects, military operations will seek to influence the population where these wars are being fought. Soldiers will need to be trained on cultural aspects of communities and will need to exercise some degree of soft power to be effective. There is not a formula that exists for this type of warfare, and each case will be elegantly unique, yet the shift will involve the adoption of many existing information operation techniques used on a much larger scale.

Russia and Information Operations

Russian information operations are rooted in concepts comparable to the U.S. definition, including similar core capabilities such as computer network operations, electronic warfare, and psychological operations. In 2011, the Russian Ministry of Defense concept for future information operations defined information warfare (информационная война) "as the ability to . . . undermine political, economic, and social systems; carry out mass psychological campaigns against the population of a state in order to destabilize society and the government; and force a state to make decisions in the interest of their opponents" (Allen & Moore, 2018, p. 60). The U.S. often reserves information operations for times of conflict, yet Russia does not hesitate to

employ these techniques during peacetime. Unlike the United States, Russia believes information operations to be a decisive tool rather than a supporting element (Allen & Moore, 2018). The Russian modern principles stem from the special propaganda, or spetspropagranda, and disinformation, or dezinformatsia, employed by Joseph Stalin (Charters, 1985). While, propaganda at the time of Stalin was intended to convince the Soviet population of an accepted "truth," propaganda in the time of Vladimir Putin now targets outside populations, and fuels both sides of arguments in an attempt to sow distrust and disinformation. As a part of these campaigns to achieve political goals without the use of military force, Russia has developed methods of deception under the time-honored concept of Maskirovka.

Maskirovka

The term maskirovka loosely translates to disguise, but it covers multiple aspects of deception aside from concealment. These include imitations, decoys, denial, and disinformation. The term represents structure of actions taken to prevent the enemy from effectively collecting intelligence and reconnaissance. This forms a struggling dichotomy between the advances of technology and advances in deception tactics to limit collection. The Soviets have long understood the importance of the element of surprise in the basic conditions for success in battle. Maskirovka originated as a military doctrine, dating as far back as the era of Catherine the Great, but its use has spread to all aspects of Russian government. Russia's actions toward enemies are not limited to the confines of the battlefield. The whole-of-government approach requires each sector contribute to masking the nation's true intentions. This allows them to keep their enemies off-balance. The Russian deception practitioner may demonstrate false strength in certain areas

while at the same time, prevent information collection about their weaknesses. The methods of the doctrine have been continually updated to remain relevant with advances in technology. Some authors maintain that the shift from military to an all government approach warrants a new term to describe it, Maskirovka 2.0 (Roberts, 2015). It should be argued that the current iteration is not dramatically different from the principles applied in its conception. While Maskirovka may be applied with new methods, the principles remain the same. Each iteration of Maskirovka has three common goals: cause a distraction for the enemy, mask the true operation, and provide disinformation. There are new tools to apply these goals such as coercion, media manipulation, and cyber-attacks, but the foundational ideologies stand. The evolution of Russian deception has changed to match each facet of the government, now featuring geopolitical goals in unison with the existing military goals.

Active Measures

The concept of active measures can be traced back to the 1920s, where former KGB Maj. Gen. Oleg Kalugin described them as activities specifically designed to "weaken the West, drive wedges in the Western community alliances of all sorts, particularly NATO, [and] to sow discord among allies" (CNN, 1998). While active measures traditionally fall under the broad umbrella term of influence operations, these politically driven actions involve disinformation or propaganda and can even extend to violent methods. During the Cold War, the USSR took actions to discredit and undermine U.S. agencies and departments, incite racially charged violence, and release false information about private organizations (CNN,1998). Before the 1984 Los Angeles Olympics, KGB officers mailed falsified letters from the Klu Klux Klan to the

Olympic committees of African and Asian countries in an attempt to cause outrage and controversy (Aceves, 2018). While the USSR no longer stands, the notion of active measures remains. The goal of its Russian successor is to disrupt and discredit Western democratic principles.

Reflexive Control

Reflexive Control is a term used to describe the practice of predetermining an adversary's decision so it aligns with Russian interest, by altering the adversary's perception of the world (Kasapoglu, 2015). By shaping an adversary's perception, Russia is able to have varying degrees of influence on their actions, with a goal of neutralizing the opponent's advantages. The term "reflexive control" is mostly used by Western nations to describe Russia's tactics, however Russia describes it as "perception management" (Giles, 2016). Through these types of information operations, Russia will display, act on, and convey motives and minor actions that cause others to react in a certain, desired way. The adversary will act on their own accord based on the perception Russia has surrounded them with. In general, there are five methods to achieve control of an opponent's decisions: By applying pressure of force, assisting the opponent's formulation of the initial situation, shaping the opponent's objectives, shaping the opponent's decision-making algorithm, and the choice of the decision-making moment (Giles, Sherr, & Seaboyer, 2018).

On a smaller scale, this strategy can be seen when a lawyer cross examines a witness, providing questions and phrasings that lead a witness to decisions and responses that are desirable to the lawyer. The application of this method is a persistent onslaught to multiple

cognitive functions of decisions makers (Giles, Sherr, & Seaboyer, 2018). A key characteristic is the need to tailor false information to each target, and continually adapt it based on the target's response and reaction (Giles, Sherr, & Seaboyer, 2018). There is a form of military art rather than military science associated with reflexive controls, wherein the influencer must provide enough information, in a non-obvious manner, that will lead the adversary to logically conclude a desired theory and act on it. As opposed to solely providing disinformation, Russia must take into account the logical processing of the adversary, as well as cultural, emotional, and psychological frameworks where decisions are made (Giles, Sherr, & Seaboyer, 2018). Troublingly, these methods have been designed to apply to the tactical, operational, and strategic levels and have been employed through multiple centuries (Giles, 2016). The Russian-Crimean conflict provided examples for each level. At the tactical level, the reflexive control provided a cover of deception for deployments and maneuvers of Russian forces when taking control of critical positions (Kasapoglu, 2015). Operationally, the military buildup along the border not only pinned down Ukrainian forces, but also confused Kiev leadership and the West about the true scope and nature of Russia's intentions (Kasapoglu, 2015). These methods framed the impression of a possible invasion and gave Russian control over the level of escalation. Throughout most of the conflict, the troops on the border served as a distraction from the Russian activities taking place within Ukraine (Giles, Sherr, & Seaboyer, 2018).

Reflexive controls are not solely meant to target high-level decision makers, but can also target the general population. By exploiting traditional democratic principles, Russia can target the fact that Western democracy uses elected officials. Due to mass media coverage, the elected officials and general population often have the same channels of information. This flow of information can be tainted, and while the elected officials may disregard the information, there is

a chance of the general population calling for action and providing increased attention to the desired reflexive action. While the main goal is to push the adversary to a predetermined goal, an alternative is causing paralysis in decision-making, which can prove to be just as beneficial.

Operation Anadyr and the All-of-Government Approach

There are multiple instances of the USSR and Russia implementing information operations throughout history, but Operation Anadyr during the Cold War exemplifies its progression as a means of influence and applying deception on a strategic scale. The operation was conceived when NATO and the United States moved fifteen nuclear missiles into Turkey on June 1, 1961. Turkey shares a border with the Soviet Union, and the missiles' range could strike nearly any location in the country. Despite claims that the missiles would not be used as a first strike option, the Soviet leader at the time, Nikita Khrushchev, could not ignore their presence. The placement of the missiles led to the development and planning of Operation Anadyr. Seeking to apply the same pressure and risk that the existence of the Turkish missiles caused to the Soviet Union, Khrushchev looked to move missiles and troops to Cuba. Cuba is less than 200 miles from the United States, and the Soviets possessed nuclear capabilities that could reach Southeastern states from that distance. Knowing that an overt mission to ship missiles to Cuba would be met with political outrage that could lead to a threat from the Turkish missile sites, a deception plan was conceived. In its early stages, knowledge of the deception was kept the absolute minimal number of people as possible. Secretaries were not allowed in these meetings, and every aspect of the plan remained hand-written (Hansen, 2002). Once the plan was

cemented, there were no signal communications, not even coded messages, only hand-carried messages to senior officials who were directly involved.

The first step of the Anadyr plan was to get Cuba to agree to house the nuclear weapons. Multiple delegations were sent under the cover of agricultural experts (Hansen, 2002). The Cubans were hesitant, and had to be convinced that the U.S. was too large a threat and that the nuclear missiles offered them protection. They wanted to make a public statement about the missile shipments, but Khrushchev successfully convinced them to conceal the details.

The next step was developing a cover story. This came from the operation's name, Anadyr. Anadyr was a port town in the northern USSR, and the easternmost town in the country. Upon hearing the name of the operation, any lower ranking military members or western spies would believe the mission was going to happen in the desolate region of the Northern USSR. Troops were led to believe they were heading to the frigid north by being equipped with parkas, skis, and other winter gear (Hansen, 2002). When it came to the actual shipment, the missiles were loaded under the cover of night and with the tightest security. The troops that were being loaded onto the ships were kept nearby, not allowed to leave the facility or communicate with anyone outside of the area. The military hardware was shielded by metal sheets to prevent infrared detection and various vehicles such as trucks, tractors, and harvesters were stored on the decks of the ship in order to display this shipment served an agricultural purpose. Troops were only allowed topside at night, in small groups, and kept under the ship in sweltering conditions during the day (Hansen, 2002). Ship captains were not told the exact destination of the cargo, but were given sealed envelopes that had the target port, which was only to be opened at certain geographic coordinates. The captains were instructed to take all evasive actions possible, and if that failed, destroy all military and state documents, secure personnel, and sink the ship.

Next came the use of diplomatic deception. In order to reduce the U.S. reconnaissance efforts on their traveling ships, Soviet delegates suggested the U.S. recon presence in international waters was a form of harassment and pushed U.S. officials to stop these flights to allow for better relations (Garthoff, 1998). In press conferences, Soviet representatives stated multiple times they had no intention of turning Cuba into a forward strike base and that they were merely supplying defensive measures to the Cubans (Hansen, 2002). The Soviets had earned enough trust from Washington, that it required definitive proof in the form of U2 surveillance photos before John F. Kennedy took action.

This campaign had two prongs, military and diplomatic deception. The Soviets knew they would not have any leverage over the U.S. if they became aware of the missiles before they were operational, therefore the vast amount of resources expended on this deception were deemed necessary. There could not be a single weak link in this plan or it could spell nuclear war. So, the Soviets applied Maskirovka principles to other sections of the government and political interactions. This all-government approach created a nearly successful operation that could have shape geopolitics for decades to come.

Given the advancements of technology between WWII and the Cold War, intelligence collection was at a new peak. This meant that the deception methods had to be even better to defeat them. This operation had a bottom-up approach that ensured each level of the plan would be given the greatest chance for success. The fewer individuals allowed to know about the missiles, the less likely the enemy would discover their plan. Therefore, the Soviet's method for disseminating information only through trusted couriers and in hand-written fashion ensured that the enemy would not intercept a communication or overhear a rumor about it. At the lowest

levels, soldiers believed they were headed towards Anadyr, and by deceiving them, they could not potentially leak the plan.

The Soviets established contingencies to allow the government deniability if their covert action was discovered. It would require critical proof for the U.S. to risk accusing the Soviets of this action, proof that the Soviets nearly hid entirely. By convincing the U.S. to lower their recon over maritime trade routes, the Soviets had used an influencer previously unseen, overt diplomatic action. In the hindsight of the operation, their intentions are clear, but at the time, their request had seemed reasonable to their country's motives. Without the advanced recon of the U.S., the troops headed to Cuba could remain under the hull during the day and surface at night, giving the United States an extremely low likelihood of detecting their actions. The ability to shape U.S. actions without the use of the military opened the door for future Soviet deception. JFK had established some degree of trust, and put faith into direct communications with the Soviets over their intentions with Cuba.

In most aspects, this deception was a success. It had successfully combined a disjointed military and geopolitical deception. The Soviets managed to deliver a massive amount of equipment, weapons, and troops to their U.S. neighbor. The plan's only downfall came at the hands of the advanced technology and collection methods of the United States. Their deception had been so successful up until that point, that it required hard evidence of what the Soviets were doing to convince the U.S. president.

Chapter 3

Deception

Deception has existed as long as warfare has, but the formal theory surrounding it is a more recent development. Formal deception analysis, in regards to military science and international affairs, began after WWII (Bennet & Waltz, 2007). Once the war had concluded, scholars and historians began reconstructing the various deception operations and methods used by military leaders. Through the recreations, they were able to interpret the actions, motives, and intent of the deception, but studying this did not help to explain why the deception proved successful. This prompted the further study of cognitive, social, and psychological aspects behind those who had been deceived (Bennet & Waltz, 2007).

In 1969, Dr. Barton Whaley attempted to produce a unified source on the detection and analysis of deception during war. He believed deception had the main goal of achieving strategic or tactical surprise on the battlefield and should be sorted into three types: diversions, camouflage, and disinformation (Bennet & Waltz, 2007). After reviewing military deception operations, Whaley identified three major components: The alternative goals or objectives of the deceiver, the alternative expectations of the victim, and the techniques by which the deceiver's goals are achieved and victim's expectations manipulated (Bennet & Waltz, 2007).

During the 1980s, Donald Daniel and Katherine Herbig created a new definition, the deliberate misrepresentation of reality done to gain a competitive advantage (Bennet & Waltz, 2007). This definition allowed for a wider interpretation of possible deception operations and did not limit them to acts performed by the military. Rather than simply obtaining benefit from the target's

surprise, Daniel and Herbig offered three degrees of goals for the deceiver. The first immediate goal is to condition the target's beliefs, the intermediate goal is for the deceiver to influence the targets actions, and the ultimate goal is for the target's actions to benefit the deceiver (Bennet & Waltz, 2007).

There has been a plethora of research since WWII, and there is a general consensus surrounding some topics, while others like structure and vocabulary remained diverse. Michael Bennett and Edward Waltz reviewed previous models and research and created what they thought to be a somewhat unified method for describing the elements of deception. These elements include the deception objective, deception story, deceiver, target, deception channel, channel message, desired actions, and the intended effects. Each are further described in Table 1.

Table 1. Elements of Deception

Element	***Description***
Deception Objective	The desired result of deception campaign, usually expressed in terms of what the target is to do or not do.
Deceiver	An actor, individual, or group arranging the deception campaign.
Target	An individual or group that is the focus of the deception operation.
Deception Story	A scenario that outlines the deceiver's actions that will cause the target to adopt the desired perception, take the requisite action, and lead to a given effect. This serves as the story board of the deception campaign and displays it as a narrative.
Deceiver's Actions	Actions taken by the deceiver to assure each phase of the deception campaign is successful.
Means & Methods	Tools, systems, and products used to carry out the deception.
Deception Message	The narrative or information the target is to perceive which warrants the desired action or reaction.
Deception Channel	The pathway for the deception message to travel from the deceiver to the target.

Cognitive Bias/Exploitable Trait	This is the element that makes the message or deception believable in the eyes of the target. This requires understanding of the target to find such a weakness.
Element of Truth	This is a compliment to the cognitive bias by increasing the believability of a given deception.
Desired Actions of Target	Action taken by the target in response to the deception message or deception stimulus.
Feedback	Process by which the deceiver is able to see progress of their deception based on the actions of the target or similar.
Intended Deception Effects	The desired outcome that stems from the target's action or reaction.

Chapter 4

What Makes Us Susceptible?

Most have heard stories of scammers, such as the famous Nigerian prince seeking to move his wealth out of the country. In most cases, an individual or group does not make a conscious choice whether they will fall victim to a deception operation. Victims of deception operations fall prey to cognitive pitfalls that lead toward actions that favor the deceiver. The deceiver is attempting to manipulate the perceptions of the targets, raising or lowering their suspicions intentionally, diverting their attention, or inciting confusion. This intentional manipulation has a focus on shaping biases. In terms of everyday usage, bias is the predisposition to judge people, ideas, or situations based on an individual's point of view. (Bennet & Waltz, 2007). The three main categories analysts should focus on are: cultural and personal bias, organizational bias, cognitive bias (Thompson, Hopf-Wichel, & Geiselman, 1984).

Cultural bias is the result of applying one's own culture when judging events or individuals. This predisposition is based on the beliefs, morals, customs, and habits that stem from environment the victim of bias is accustomed to. There are cultural norms that vary from region to region drastically. In the United States, though separated by only a few miles, certain regions utilize a different lexicon when describing everyday objects such as the variations between soda, pop, and Coke. This is an innocent example, but when the concept is applied to larger regions of the world, a cultural norm in the United States may be deemed incredibly disrespectful in another country. It is common for one experiencing an event to want to apply their own lens to it, but this can lead to misinterpretations or altered perceptions. This is a subcategory of bias called mirror imaging and often occurs by attempting to explain events or fill informational gaps with personal experiences. When comparing the military strategies of Western Civilization to the rest of the world there is a clear difference in the norms of the culture. Western militaries have mostly emphasized high levels of force and technological capabilities, while discrediting deceptive ambushes and strategies they deem dishonorable (Bennet & Waltz, 2007). This varies greatly from China and Russia, who have embraced deceptive military practices as means of strategic advantage. China has been developing the philosophical principles surrounding deceptive warfare for over 2,000 years under the teachings of Sun Tzu. If U.S. strategic planners did not combat their cultural bias, they would assume these countries would wage war in the same manner the U.S. does. A deceiver can target this bias by providing facts that compliment to the accepted, subconscious norms of the target's society, effectively limit their perception of events.

Personal bias is caused by personality traits and firsthand experiences that affect the individual's world view throughout their life (Bennet & Waltz, 2007). There are four variables

that affect the degree to which an individual allows personal experience to affect their predisposition: firsthand experience, whether the experience occurred in early adulthood or career, the importance of consequences to the individual or their nation, and the extent to which the individual has been exposed to events that facilitate alternative perceptions (Jervis, 2017). Preconceived beliefs are resilient to change, even when faced with contrary information, allowing an opportunity for deceivers to exploit them. Personal traits such as overconfidence can lead to devastating failures when deception is involved. Overconfidence can specifically create a feeling of security and guaranteed success leading to the underestimation of the adversary.

Organizational bias is created from the goals, mores, policies, and traditions of the specific organization the individual works for, typically affiliated with large bureaucracies (Bennet & Waltz, 2007). Given the structure of the U.S. government, the abundance of bureaucratic elements allows for an array of targets for a deceiver. As large organizations became the norm, they developed standard operating procedures as means of efficiency (Bennet & Waltz, 2007). During normal conditions, the procedures are beneficial, but when deception is introduced, these procedures could prove detrimental. In regards to information sharing, there are guidelines and processes to facilitate the flow of information to those who need it. The individuals in charge of managing the flow of information are called gatekeepers, and they are able to determine if the information will be spread to separate levels or the public. This key role can become the target of the deception as they can control a deception message reaching other parties. To examine the dangers of this bias one should look at the intelligence surrounding the Japanese attack on Pearl Harbor. The attack was not anticipated, yet a few individuals had seen communications regarding a potential assault prior to the attack (Wohlstetter, 1962). The sharing of information was a problem at this time, and this event highlighted it. It is rarely an issue of

having enough intelligence prior to an event, but rather the sharing and fusion of the intelligence that becomes an issue. Each organization within the bureaucracy may be required the coordinate and share in the goal of a common mission, but they will have prime interest in their organization's success, power, and goals. Reports produced by certain parties or groups may involve some editorialization to achieve their desired outcome. For some military reports, they could overstate the current threat in hopes of increased funding. Parties could attempt to push an agenda not directly related to a project with a specific goal in mind.

The concept of cognitive bias relies on heuristics. Heuristics were defined by Amos Tversky and Daniel Kahneman to refer to the process in which individuals will reduce complex mental tasks, especially under conditions of uncertainty, unavailability, and indeterminacy of important information (Tversky & Kahneman, 1974). Tversky and Kahneman identified three broad heuristics: representativeness, availability, and anchoring and adjustment; each was associated with a set of biases (Bennet & Waltz, 2007). They described the representativeness heuristic as, "A person who follows this heuristic evaluates the probability of an event or population by the degree to which it is: (i) similar in essential properties to its parent population; and (ii) reflects the salient features of the process by which it is generated" (Kahneman & Tversky, 1972, p. 431). This means that if event A resembles event B, an individual is more likely to believe event A is a member of event B's class. This heuristic is often present in profiling, when an individual believes a person to be a part of a nefarious group due to the resemblance of the person to that group. The point being they are trying to fill informational gaps based on generalizations of groups and data. The availability heuristic is a mental shortcut that relies on the ease with which an individual can recall an event that the resembles the uncertain event they are experiencing. The more easily available instances are likely to have a stronger

impact on the individual's belief than the actual data or frequency. The anchoring and adjustment heuristics give increased significance to the first piece of information processed. The starting point holds greater value, and if presented with updated information, the adjustments are insufficient (Bennet & Waltz, 2007). Once the analyst has become focused on this point, it is hard to move away from it, even if the information is contrary. Given the mental shortcuts and biases present in individuals, deception planners have learned it is easier to reinforce a target's preconceived notions and prior beliefs than it is to convince the target of an alternative they are not predisposed to (Heuer, 1981). Richards Heuer produced three general conclusions about the effect of cognitive biases: (i) people do not do a good job at generating a full set of hypothesis; (ii) there is a tendency to view information as supporting, contradicting, or irrelevant to a hypothesis; (iii) analysts can be fixed in a mental set they have created that resists the impact of discrepant information (Bennet & Waltz, 2007).

Chapter 5

Social Media's Role in the Disinformation Process

Social media is a concept that has existed for multiple elections prior to 2016, yet during the last election cycle, its impact reached magnitudes never seen before. While the concept of social media was explored in the late 1990s and early 2000s, social media had its largest impact on daily life with the mass cultural adoption of smartphone technology during the late 2000s. Prior to smartphones, use of the Internet was, in most cases, reserved to a user's computer. When the technology became available, a new market was introduced, smartphone applications. The companies that ran to fill the need were not entirely unique or independent from earlier Internet-centric companies. Twitter is a prime example of an existing company who adapted to fill the market. Twitter became a standalone company in 2007, and while only on the Internet, received a high level of popularity. In 2010, Twitter released their official app on the app store for the iPhone, iPad, and Mac (Miller,2010). The company saw its usage numbers skyrocket, and eventually was named the tenth most downloaded application of the 2010 to 2020 decade (Rayome, 2019).

During the Internet boom, traditional, print news reporting sources began to see a decline. With print sales dwindling, news outlets had to adapt and began to embrace the potential of social media. The main purposes for implementing the likes of Twitter include disseminating news, marketing stories, and establishing relationships with news consumers (Broersma & Graham, 2012). Twitter had previously limited its content to 140 characters, which brought into question the ability of a news source to fully cover an event. This would require reporters to be precise and succinct with their language and potentially limit crucial details of a developing story. Often times only a headline will be tweeted, followed by a link to a full article. However,

in time sensitive events and emergency, sometimes civilians can become journalists. In the moments immediately following the 2009 crash of US airways flight 1549, a passenger of a nearby ferry was able to take and post a picture of the downed jet floating in the river before any news crew arrived at the scene (Murthy, 2011). This could appear to be a resource for news outlets, first responders, and potentially affected civilians; however, there are dangers and pitfalls when utilizing unverified sources for seemingly credible news. The picture of the downed flight the individual shared could be circulated thousands of times within the first minutes before the story has been confirmed or denied. Through the process of "retweeting" a Twitter user can see posts from accounts they do not actively follow. A celebrity might retweet a topic they are concerned with, which may not be factually accurate, and disseminate that false information to others. This has led to numerous hoaxes that spread from account to account.

The most recent viral hoax involved celebrities and some politicians posting a disclaimer on the Facebook owned company Instagram stating they do not accept the new terms and conditions to make all photos public (Palmer, 2019). The hoax message claimed this was the last day possible to prevent Facebook from using their photos. A screenshot was taken of the post and reposted an incredible amount of times after that. The transmission of hoaxes, fake news, and disinformation can mirror the spread of a viral infection. The transmission rate can become exponential as more accounts share the content. With the amount of potential time spent on social media, individuals need to be cautious of disinformation and not base their actions off of uncredited or illegitimate sources.

Chapter 6

Anatomy of the 2016 U.S. Election

Introduction

The 2016 United States presential election was disrupted by Russia via influence operations meant to spread disinformation, sow political discord, and undermine the electoral system. The candidates Hillary Clinton and Donald Trump provided Russia an opportunity to target citizens of the U.S. and drive them further toward political polarization. Russia did not push for the election of a particular candidate. This is a common misconception surrounding the data analyzed via Twitter and social media, as there are large amounts of Russian data supporting Trump and disparaging Clinton. However, the data also demonstrates Russian driven support of Clinton and berating of Trump. By playing both sides of the aisle, Russia was seeking to incite political discord.

The Internet Research Agency (IRA) is based in Saint Petersburg, Russia and began operating in 2013 (Chen, 2015). The IRA has been known for spreading false information on the Internet, previously employing hundreds of Russians to post pro-Kremlin propaganda under false accounts to simulate massive support (Chen, 2015). The IRA is known as a "troll farm." This agency focuses on both domestic and foreign targets, and prior to their involvement in the election, had perpetrated multiple hoaxes via social media (Chen, 2015). Robert Mueller's investigation led to the indictment of the IRA as the central component to the election influence operation.

IRA-linked social media accounts were discovered throughout Facebook, Twitter, Instagram, and Google (Boatwright, Linvill, & Warren, 2018). The accounts portrayed themselves as

American citizens trying to promote divisive issues, but were actually Internet trolls attempting to create a political rift. Within the IRA, there are over a thousand living individuals operating the false accounts around the clock (DiResta et al., 2019). They have reached 126 million Facebook users, at least 20 million Instagram users, 1.4 million Twitter users, and have contributed over 1,000 videos to YouTube (DiResta et al., 2019). The scale of the IRA operation was unprecedented, setting a new standard with its magnitude.

2016 Russian Influence Operation Campaign

The influence operation can be examined through the lens of the Elements of Deception framework discussed in Chapter 3.

Deception Objective: Create U.S. domestic and political discord.

Deceiver: The Internet Research Agency (IRA) acting as a proxy of the Russian Government

Target: Multiple groups were "targeted" during this campaign, most prominent included: Black American Voters (number 1 target demographic), Hispanic Americans, Women voters, LGBTQ, the NRA, Vaxxer & Anti-Vaxxer groups, Conservatives and Progressives amongst others. Additionally, multiple hot-button topics were targeted including: Black Lives Matter, Blue Lives Matter (perceived opposition), Vaccination, 2nd Amendment, Immigration, "the Wall," Universal Health Care, Homelessness, Abortion, Military Spending, the Global War on Terrorism, WikiLeaks, DNC Email Hack, and others.

Deception Story: This deception campaign spanned a period from 2013 (well before Trump was in the presidential picture) through the inauguration in January 2017 and beyond. The Russian Internet Research Agency created thousands of social media accounts, micro-

targeted special interest groups and selected voter demographics (targets) with messaging that appeared to originate from opposition groups in order to sow general discord and unrest (objective). Using a combination of human and bot-generated micro-messages, (methods & means) across a wide range of social-media platforms (channels), the troll farms pushed targeted messaging that appealed to the emotional connectedness (cognitive bias) of the targeted group for the purpose of eliciting a response in kind against the opposition (perceived) sender group. By monitoring the reaction (feedback) of real users (and main-stream media), the trolls were able to adjust to the tenor and frequency of messaging from both sides and ratchet up the messaging when needed. One of the desired intermediate objectives of the micro-targeted messaging campaign was to set the stage for a self-sustaining social media exchange between opposition groups. In this case the messaging (tenor and volume) has reached a level such that the trolls no longer need to feed the system directly. A key aspect of the IO campaign included the recruitment of tacit participants (unknowing assets) who would insert original content, organize action, or retweet content from Russian influencers, including things like videos of police abuse, or spreading misleading information about how to vote and who to vote for. A gold standard target of this type was someone with a celebrity status, especially when their social-media followers joined the fray.

Deceiver's Actions: Identify Groups and Topics, Establish Fake SM Accounts, Construct Micro-Targeted Messaging (from both sides), Monitor Response, Adjust Messaging and Elevate as necessary toward achieving a self-sustained state.

Means and Methods: Weaponized social media using platoons of social-media engineers, augmented by botnets to conduct micro-targeted messaging across a wide span of hot-

button topics. Further augmented by tacit participation and by taking advantage of targets of opportunity (real-world events that reinforced ongoing dialog).

Deception Message: Politically charged content and information passed via a Deception Channel (Social Media) to be picked up by the Deception Target (targeted groups/persons) and which leads to a given understanding (perception), action or decision by the Target.

Deception Channel: Spanned the entire Social Media Space, but also relied on Main-stream media, and other forms of reporting to extend the messaging, particularly when a reinforcing event emerged or when a personality or celebrity voice was added to the mix.

Cognitive Bias/Exploitable Trait: In many cases, all that was needed was a prompt that fed on already existing beliefs or emotional attachments to a cause. Messaging keyed on micro-aggressions such as victimhood, disenfranchisement, prejudice and injustice. Messaging formed around micro-aggression tended to be some of the most aggressive and hateful. Some were invented out of whole cloth, and others that were in response to a real-world occurrence – a prime target of opportunity. The troll farms monitored for a real-world event (school shooting, police violence against a person of color, or other attention getting event) to use as an example and reinforce the belief that micro-targeting is real.

Element of Truth: For each targeted group or micro-targeted topic, the trolls used existing messaging to construct believable social-media posts reflecting an already familiar set of views and counter-views. In many instances, they constructed both sides to play against the middle to widen the divide.

Desired Actions of Target: Started at the issue level and across multiple topics, but was segmented in such a way that no single-issue group recognized the pattern of

manipulation happening across the wider range of issues. When planned reactions did not materialize as expected (force or frequency), then the troll provided the reaction themselves, elevating the level of hateful discourse at each step. Over time, reactions became self-generating with real hate being heaped from both sides.

Feedback: Was garnered by monitoring social-media response for each targeted group and micro-targeted topic and adjustments made accordingly.

Intended Deception Effects: Polarization of American political atmosphere. Disruption of the democratic process through division and gridlock.

Analysis of Internet Research Agency Tactics

The Russian interference campaign consisted of three distinct forms:

1. The targeting and attempted hacking of online voting systems and voting infrastructure.
2. A cyber-attack on the Democratic National Committee and subsequent leaking of Clinton campaign emails.
3. Massive scale social influence via coordinated disinformation directed at U.S. citizens.

Forms 1 and 2 represent direct methods to influence the results or discredit the electoral system in place. The hacking attempts and cyber-attacks can easily be measured as successful or unsuccessful, but the third form does not fall on this binary scale. The large influence campaign consisted of two prongs: political advertising and false social media accounts. Russia has limited options to see if these account or ads had successfully influenced a voter; all they could measure were the engagement levels by real users. Data can be collected and analyzed surrounding the accounts, tweets, and advertisements, but it is impossible to quantify if a person in Nevada

changed their vote due to something they saw on social media. The third form will be analyzed in the remainder of this chapter due its novelty, scale, and intricacy.

In the years since social media's inception, targeted advertising has seen a steep increase. Through targeted advertising, consumers are meant to be given advertisements that match their interests. This is supposed to allow for a more efficient system where the personal data collected on a profile will allow for ads the user is likely to engage with. This can easily be abused by malicious actors who wish to spread disinformation or incite conflict. Since the ads are not witnessed by the non-targeted and non-vulnerable, the ads are likely to go unreported and their effects undetected (Ribeiro et al., 2019). Platforms like Facebook and Google provides a service by allowing companies and groups to spread their brand and ideas, but with little oversight and regulation, this system can be easily corrupted. The IRA was able to take advantage of this process through geographical targeting. The splitting of demographics by region served two purposes: first, targeting communities for local events and rallies, and second, targeting areas with race- and police-brutality incidents (DiResta, 2019). For the IRA, timing was very essential. Once news broke of an incident involving racial profiling, police violence, or similar, they would purchase ads in the area. They played both sides of the coin, purchasing ads for both 2nd amendment rights and Black Lives Matter. The messages were steadfast, and designed to embolden those who were troubled by the status quo.

Facebook reported the IRA had purchased close to 3,500 advertisements for over $100,000 (Mueller, 2019). The IRA had a budget that exceeded $25 Million USD (DiResta et al., 2019). With such a massive budget, there were few limitations placed in front of the IRA. The troll farm was able to deceive ad companies into believing their accounts were operated by American citizens, and the systems in place proved ineffective in identifying the true origin.

Their ads supported or opposed a presidential candidate and provided messages that conflicted with the status quo (Mueller, 2019). These ads were meant to push extreme left and right leaning messages, further expanding partisan divide. The IRA was also able to create and promote physical gatherings, rallies, and protests through social media. Some accounts, without revealing their Russian association, communicated with Trump campaign representatives and activists to coordinate political activities such as rallies (Mueller, 2019). The rallies were not limited to Pro-Trump, such as an account called “Black Matters” calling for a “flashmob” (Mueller, 2019). The goal of these rallies they organized was to create an echo chamber of ideas, wherein participants leave the event further fortified in their beliefs. By creating groups and sending private messages, IRA members were able to move their influence from cyberspace into a physical gathering of like-minded individuals.

The largest impact of the campaign came from the overwhelming amount of social media accounts the IRA produced. On Twitter they had approximately 10.4 million tweets (~6 million were original content) spanning 3841 accounts, roughly 1100 YouTube videos contained within 17 account channels, nearly 116,000 Instagram posts across 133 accounts, and 61,500 unique Facebook posts across 81 Pages (DiResta et al., 2019). Having mountains of content does not guarantee real users will see it. Based on the data the companies provided, there were ~77 million engagements between 126 million affected individuals on Facebook, ~187 million engagements between 20 million affected individuals on Instagram, and ~73 million engagements on their original Twitter content engaged by 1.4 million individuals (DiResta et al., 2019).

Some researchers have divided the Twitter accounts into four categories. The newsbots had usernames like @PittsburghToday or @LASports and tweeted news articles from the regions

they claim to be from, the “right-leaning” and “left-leaning” accounts that attempted to resonate with individuals who find themselves far from the center of the political spectrum, and repurposed accounts were from traditional botnets that served to amplify content with retweets and likes but do not produce opinions or content of their own (DiResta et al., 2019). Many of the accounts were automated to produce tweets or content at the same time. Some received human management though, and were likely the accounts with the most followers, influence, or connections as they would be the most heavily scrutinized.

The newsbots, right-leaning, and left-leaning accounts would produce content targeted towards specific audiences about various controversial issues such as immigration, abortion, healthcare reform, and the Black Live Matter movement. First-round messages promote an accounts agenda, for example, supporting right-leaning issues and condemning left-leaning issues. In round-two, a sequence of bots then begins a heated series of discussions and comments on the content. Eventually, a genuine, living account will join the fray either to defend their side’s content or provide opposition. This living account may receive replies from bots, but eventually, once enough attention has been drawn to the content, another living account joins the discussion, allowing the system to acquire a self-sustaining quality. As more legitimate users join the discussion, the less the botnet is needed to provide replies. Users can now be spurred into replying because they find the previous comments so objectionable or defendable. Effectively, the botnet has created a self-sustaining loop of divisive comments and responses. In this sense there is no discussion about the issue, rather an echo chamber where biases are strengthened.

In order to maximize the influence these bot accounts possessed, the IRA had to understand and exploit the culture and language of social media users. False stories, disinformation, and clickbait have existed long before the 2016 election. Social media and

content-based companies thrive on providing eye-catching headlines to ensure consumers engage with their content, with a goal of receiving “clicks” and views. Emerson Spartz launched a media company that repackaged crowdsourced viral web content under titles that were meant to garner attention (Marantz, 2019). Titles could include something similar to, “The 10 Best Main Streets in California. #4 Surprised Me.” The title had both information on the content and also an incentive for the viewer to stay engaged. The company makes money based on the user engagement levels, and they are incentivized to develop deceptive practices to increase them. These methods can be adopted by malicious actors. While studying what makes items trend, the IRA was able to ensure viewership for their underhanded messages. Instagram proved to be the most effective in garnering attention, as 40% of its accounts had over 10,000 followers and twelve accounts had over 100,000 (DiResta et al., 2019). This number of followers puts them in the field of the so-called “instafamous” and influencers that shape the perceptions of social media users. The IRA had a willing audience, ready to consume whatever content the agency believed would create political unrest in the United States.

Chapter 7

Notional Framework for the 2020 U.S. Election

U.S. Response to 2016

In the aftermath of Russia's influence operation, the United States has attempted to take actions that will hinder any foreign nation's future efforts in undermining elections and weaponizing social media. Action has been taken by both the federal government and private companies to fortify election infrastructure. In response to influence operations, former Director of Homeland Security, Jeh Johnson, designated election infrastructure as critical infrastructure. This elevates its cybersecurity and protection priority within the National Infrastructure Protection Plan (Johnson, 2017). This response indicates a national effort to harden election systems and prevent future interference. The United States federal government is recognizing the danger and likelihood of this threat by including it within the Director of National Intelligence's Worldwide Threat Assessment. The director acknowledges Russian efforts to aggravate social and racial tensions, undermine trust in authorities, and criticize anti-Russian politicians (Coats, 2019). The threat assessment suspects Russian efforts to interfere in our political system will be more targeted in the future (Coats, 2019).

Private companies have had to take action in the wake of the 2016 election. Companies, such as Facebook, had to redevelop company policies and procedures that were exploited by foreign nations. Upon seeing the harm and disinformation their platforms could spread, these social media giants sought to analyze their role in the process and mitigate the misuse of their resources. Facebook released a report detailing how they were handling the information operations taking place on their platform. They identified three major features of Facebook that

had been used by malicious actors: targeted data collection, content creation, and false amplification (Weedon, Nuland, & Stamos, 2017). Targeted data collection sometimes involved phishing attacks and spreading malware to collect information on targeted individuals (Weedon, Nuland, & Stamos, 2017). The creation of false or real content is difficult to regulate on social media platforms because the companies want to avoid becoming gatekeepers of information and seek to allow to free speech whenever they can. The reporting of fake media on these sites has improved, but it likely the most vulnerable aspect of social media. False amplification allows for the information operator to increase the range at which their message is spread. Through false amplifiers, a fake news story can be circulated at an exponential rate. By creating a plethora of fake accounts, the deceiver can target and coordinate different pieces of disinformation with distinct goals of promoting the issue, sowing distrust in political institutions, or spreading confusion (Weedon, Nuland, & Stamos, 2017). Private companies cannot fully control how each user employs the platform, but by understanding the issues surrounding it, they have better chance of slowing information operations in the future.

A hypothetical gaze forward to the 2020 presidential election might consider the probability of a reinvigorated Russian information campaign. Three categories of IO actions in this hypothetical framework are posited: first, Russian actions may maintain the status quo they established in 2016. Despite the U.S. response to the election, Russia may believe there is no need to change their strategies and their goal can achieved with similar methods used 2016. Second, Russia may seek to escalate their efforts from 2016. An escalation could occur for two reasons: the U.S. efforts to secure the election could be successful in limiting Russian impact or they wish to amplify the disorder they created in 2016. Third, Russia may believe they have proven the viability of their methods, and seek to combine them with other tools to achieve a

new goal. For this to be true, Russia would have a broader goal in mind than causing political discord in the U.S. and would employ an all-of-government approach to achieve it. The sections following will explore non-mutually exclusive hypotheses surrounding the actions and intentions of Russia during the 2020 presidential elections.

Hypothesis – 1: Targeted Presidential Candidate

Title: Russia utilizes social media enabled information operations in order to support the election of a specific presidential candidate.

Objectives: Russia seeks to directly influence the outcome of the presidential election. They will be seeking a white house that either favors Russian global objectives, can be manipulated to support Russian objectives, or would prove to cause U.S. domestic discord and be self-destructive toward U.S. global politics.

Means: This goal would employ media enabled information operations and be an escalation of the operations seen in 2016.

Scenario: Russia will supply support for the candidates within the field they would like to see elected. They will provide opposition by exploiting weaknesses of candidates they believe will hinder Russian goals. Once the field is narrowed down, they will shift their narrative, if Russia's favored candidate has dropped out, to allow for a heated Democratic/Republican National Convention faceoff for the party nomination. Thereafter, they will make the determination between the Republican nominee and the Democratic nominee, and support one candidate while undermining the other.

Indicators: Any alarming issue or misstep by a presidential candidate will be heavily circulated by IRA-run accounts in an effort to give their competitor the edge. This could include Senator Bernie Sanders suitability for office after news was released about his heart issues. Russia may also seek to publicize the senator's backing of a communist regime's policy. The deception messages of the accounts would take that information and create additional concerns by twisting facts that have a kernel of truth. Former Vice President Joe Biden's age and mental state have become a topic of concern and Russia could manipulate clips of the former VP mis-speaking at rallies. Russia may also seek to perpetuate fears of his ties to Ukraine and potential underhanded dealings. At the time of this paper, Trump's impeachment has raised major issues about his re-election. If Russia is seeking a change in power, they will amplify these concerns in effort to harm his chances of winning in 2020.

Analysis: This hypothesis supports the idea that Russia had a favored candidate in 2016, and utilized their resources to aid in that individual's election. When examining the content of the IRA-run accounts, it should be apparent which candidate Russia prefers due to the mass tweets, posts, and advertisements. In 2016, there appeared to be Russian-linked support for both the Democrats and Republicans, but they identified more content supporting Donald Trump. It is possible there is a data issue here, as there may have been more accounts supporting Hillary Clinton that were not uncovered. This hypothesis suggests that in 2020 there will not be IRA-linked assistance to both the Republican and Democratic nominees, but rather clear lines contributing to one campaign and hindering the other.

Hypothesis – 2: Displace the U.S. as a World Power

Title: Russia employs a whole-of-government approach to reduce the global power and reach of the United States, while simultaneously elevating their own.

Objectives: Russia hopes to downgrade U.S. power status across of sectors of national power: diplomatic, informational, military, and economic.

Means: Russia will utilize a whole-of-government approach. This will involve active measures across all sectors and implement Russian instruments of national power. Russia will continue to employ IO affecting U.S. politics, but the goal of the operations has two potential outcomes. The first potential result, a president is elected that limits the affect the U.S. has on the rest of the world and promotes isolationism. The second potential result, Russian IO brings an enormous amount of attention to domestic issues facing the U.S., and U.S. leadership has to combat these issues on the homeland, rather than focus their gaze on anything happening around the world. Once the U.S. global presence has been degraded, Russia must take opportunities to demonstrate their level influence in global affairs.

Scenario: Iranians close the Strait of Hormuz and threaten to capture or sink any violators. U.S. responds by entering the Strait. A commercial ship hits a mine and the U.S. is blamed. Oil is stalled in Gulf ports, creating global economic backlash. Russia offers mine-sweeping ships to clear the straits and escorts commercial shipping to them from U.S. interference. The U.S. must deal with media that is being amplified by Russian accounts. Hoping for a shift in perception surrounding global superpowers, Russia will raise their traditional level of global involvement.

Indicators: Russia involved a regional conflict or crisis that would not have seen Russian influence in the past. This could be any type of crisis such as weather, security, natural or manmade disaster, economic, or health related. With the hope that the U.S. is tied down due to domestic issues, Russia will attempt to fill the vacuum left by a lack of U.S. intervention.

Analysis: This hypothesis relies on Russia executing a whole-of-government approach as they have historically done since the USSR. Russia would utilize any resource at their disposal to achieve this goal, including the Internet Research Agency. Russia has demonstrated a proof of concept about the objectives social media enabled information operations can achieve. The next step will be combing this new and emerging tool with other facets of their government to achieve larger scale goals. In 2016, Russian accounts did not promote foreign at the same level as domestic issues; domestic issues were the dominant targets. This can indicate a desire for the U.S. population to remain focused on their own issues to the point where they are unable to properly respond to foreign affairs. To reclaim their position as a global superpower, Russia would need to execute a large-scale operation that involves every available state-resource.

Hypothesis – 3: Expand U.S. Domestic Discord

Title: Russia makes use of social media to expand on the U.S. domestic discord that surrounded the 2016 election and push the U.S. further toward political polarization.

Objectives: Russia will continue their objective of 2016 to create civil discourse. As the divide between left and right politics grows, the democratic process in the federal government is halted.

Means: Russia will maintain the status quo and continue to use social media enabled information operations. The IRA may expand on the issues they attacked in 2016, such as targeting controversial businesses as well as other sectors.

Scenario: Russia will maintain the methods used in 2016 to promote divisive social issues, but will expand to affect business or products. They will seek to organize boycotts surrounding businesses or products based on incidents, either real or fabricated, depicting them as harmful to people, the environment, or public safety. Russia will seek to create and amplify debates that may not have been present in the past by drawing attention to unnoticed news stories.

Indicators: IRA-linked accounts will identify or fabricate stories of hazardous products. Attention will be drawn to any Green New Deal violators. Non-compliant businesses and products will have protests and boycotts organized online. As the election and debates near, issues that were raised in 2016 will resurface and be amplified.

Analysis: This hypothesis maintains the status quo established in 2016. The end result would be a heavily polarized political atmosphere, where the political spectrum expands further from the center. IRA trolls would continue to attempt to aggravate U.S. citizens into responding and taking action against views they oppose. The IRA can coordinate and implement rallies surrounding an array of issues. There is potentially no need to improve on a system that proved to be effective the last time it was implemented. The goal is to

continue to push public perceptions to further extremes and entrench citizens in their views.

Hypothesis – 4: Lead to a Dynamic Change in U.S. Democratic Principles

Title: Russia employs information operations to promote a shift in long standing U.S. democratic principles.

Objectives: Russia will escalate their information operations from 2016, and seek a major shift in baseline political structures.

Means: This objective employs media enabled information operations, but repositions the focus on foundational political values and structures. They will promote the idea that the current system is flawed and does not give citizens the voice they believe it does.

Scenario: Russia will utilize a social media campaign that promotes the rise of new party leadership. They seek to pit groups against each other, such as old versus young or poor versus wealth. This groups will vie for control over each party, eventually displacing incumbents with new representatives who oppose the traditional Democratic platform. The new platform will be closer aligned to position of radical voters who seek change. These radical ideas could include the dissolving of the electoral college or renaming of the Democratic Party to the Democratic Socialist Party.

Indicators: There will be multiple grassroot calls organized online. Some will seek representation from the likes of Washington D.C. and Puerto Rico. Others will call for leadership change in major parties, promoting candidates that oppose the status quo. The U.S. will see an introduction of bills that call for impactful changes and challenge

previous leadership decisions. Political parties will call for rebranding and lead to new party leaders. Long standing democratic principles, such as the electoral college, will be abolished.

Analysis: Russia has long been in opposition of Western democracy. After 2016, the IRA had proven they can affect a domain outside of cyberspace by coordinating rallies and events. If Russia seeks to undermine Western democratic principles, they have an opportunity to gain online support and translate it to a physical dimension. Following the 2016 election, there was an outrage surrounding the results. Although Clinton had received the popular vote, Trump had won the electoral college. Russia was able to perpetuate a message that an individual's vote was insignificant and did not impact the results. The electoral college had caused a failure in democracy and the majority was not heard. Due to this failure, the citizens must call for change in order to be heard. There has been a movement calling for the renaming of the Democratic Party to the Democratic Socialist Party. A leading Democratic Party candidate Bernie Sanders identifies as a Democratic Socialist. Many believe the party's ideals align closer to those of the Democratic Socialist countries. If inclined, Russia could coordinate grassroot support for this change. The renaming of the party could have serious implications for their future platforms and support. A domino effect would lead to major policy changes in the legislative and executive branches of government. Russia has the potential to affect more than the minds of the U.S. population and could bring about dramatic changes through the use of information operations.

Chapter 8

Summary

According to the Russian Ministry of Defense, IO is defined "as the ability to . . . undermine political, economic, and social systems; carry out mass psychological campaigns against the population of a state in order to destabilize society and the government; and force a state to make decisions in the interest of their opponents" (Allen & Moore, 2018, p. 60). Each factor of the Russian definition epitomizes their efforts to interfere in the 2016 U.S. election. Given the influential potential of information operations, the U.S. has mainly reserved IO during times of conflict. Russia holds no issue employing these techniques during times of peace and hostility. Unlike other countries that use IO as a supporting element, Russia utilizes IO as a distinct tool within its arsenal. Russia's use of deceptive practices dates back to the start of the USSR when the military doctrine maskirovka was adopted. Maskirovka laid out the foundational principles the USSR, and subsequently Russia, would use when conducting deception and information operations. Since the doctrine's creation, technology has advanced and political goals have shifted, but Russia still applies the ideology of Maskirovka to all facets of the government. With their version of IO, Russia can achieve an array of political goals without the use of military force.

Deception has existed as long as warfare has. Throughout history, nations have attempted to conceal actions, capabilities, and intentions. In a deception operation, the deceiver will take actions that shape the perception of the target and prompt actions that favor the deceiver. The means and methods of these operations may evolve over time, but there will consistently be a

deception message or narrative the deceiver is attempting to deliver to the target via a deception channel. Deception operations will prey upon the target's biases in an effort to exploit a cognitive pitfall they possess. Biases can be personal, cultural, organizational, and cognitive. Personal and cultural bias stem from an individual applying their environment, culture, and firsthand experiences when making a judgement. Organizational bias is based on the goals, polices, or traditions of the organization or bureaucracy an individual is a member of. Cognitive biases occur due to the brain's tendency to reduce complex mental tasks when under conditions of uncertainty. Each category is unique, but they can all lead to errors in judgement and decision-making.

Social media is playing an evolving role in the daily lives of individuals. For many, social media websites and applications serve as a news source. Through each platform, people can find short and easily digestible stories. Users can connect with and follow organizations, politicians, and celebrities. There is no gatekeeper on these platforms, and information is able to circulate freely. The news industry had previously resided in print format, but the Internet has forced the industry to adapt. With the speed and connectivity of the Internet, news coverage must be churned out at a rapid pace. For some smaller companies, this prevents them from fully vetting sources in an effort to report in good time. The combination of breaking coverage and a lack of gatekeepers opens opportunities for hoaxes, deceptions, and information operations.

Russia's interference in the 2016 U.S. presidential election demonstrated the scale, funding, and methods the nation is willing to utilize in order to shape global politics. The IRA, acting as a proxy for Russia, was successful in producing a diverse range of accounts, content, and advertisements. These products effectively interacted with U.S. citizens with the goal of sowing political discord. Russia was not attempting to select the U.S. President, but rather sought

to expand the divide on the political spectrum. Divisive special interest groups were targeted, and both human and bot accounts delivered content and responses. Online debates were commonplace for their strategy. The conversation would start as a bot-to-bot response, and would continue until a living account would join. Eventually, the bots would no longer be necessary, as the conversation would develop into a loop of human-to-human argumentative interaction. By utilizing social media, Russia was able to produce a massive scale, unprecedented information operation. Russia has effectively shaped a political atmosphere that has culminated with Articles of Impeachment being drawn for the President of the United States.

The United States has taken decisive action in response to Russia's 2016 information operation. Multiple investigations occurred in the wake of 2016. Eventually, indictments were drawn up to condemn the known perpetrators. The federal government has upgraded the status of election infrastructure to one of the sub-sectors of critical infrastructure. This allows for increased funding and manpower to aid in securing future elections. Private companies have had to make internal reforms to handle disinformation and foreign influence accounts. Despite these efforts, it is possible the U.S. is not prepared to handle a social media information operation similar to 2016. While the U.S. has been upgrading its potential defense, Russia has likely been progressing their methods to account for increased target resiliency. This report's hypothetical framework suggests Russia's potential IO actions in the 2020 election will fall into three categories. The first being a status quo of the operations seen in 2016. If Russia believes their operation was successful in 2016, they may not perceive a reason to change their methods. The second is an escalation of the strategies; 2016 proved this method of influence is successful and Russia may seek to provide increased resources to amplify the results. Third, having proved the viability of their methods, Russia may seek to combine these 2016 strategies with other tools in

the government's control in order to achieve a larger goal. The divide among the political spectrum has been increased and there is minimal common ground to be located. By undermining U.S. democratic principles, Russia has limited the belief some citizens place in the democratic system. The nation cannot function successfully without trust placed in the current political system. Russia will continue efforts to sow discontent in the current state of U.S. affairs and attempt to influence global politics for their own benefit.

Appendix A

Hypothesis Table

Table 2. Hypotheses for 2020 Election

	Hypothesis – 1:	***Hypothesis – 2:***	***Hypothesis – 3:***	***Hypothesis – 4:***
Hypothesis Goal	***Targeted Presidential Candidate***	***Displace the U.S. as a World Power***	***Expand U.S. Domestic Discord***	***Lead to a Dynamic Change in U.S. Democratic Principles***
Objectives	• Direct influence on outcome of the U.S. Presidential Election • An executive branch that favors or can be manipulated to support the actor	• Lower the U.S. status as a global power through all sectors associated with national power: • Diplomatic • Informational • Military • Economic	• Extension of the 2016 IO Campaign • Create civil discourse and polarization • Widen the divide between left and right	• Escalation of the 2016 IO Campaign • Major shift in baseline political structure
Means	- Information Operations • Media enabled and focused • Escalation/Continuation of the tactics used in 2016	- United, Whole of Government Approach • Active Measures ○ Russian Instruments to display their national power	- Information Operations • Media enabled and focused • Will expand beyond the candidate field to target the business sector opposition members	- Information Operations • Media enabled and focused • Focus on and target foundational political values and the issues with the structure

		○ Chinese comprehensive national power		
Potential Indicator	• Bernie Sanders health concerns raise concern of his vitality in office • Joe Biden's age, mis-speaking in debates/interviews, family ties to Ukrainian scandal • Donald Trump impeachment process	• Regional crisis prompting Russia/China intervention • Could be weather, security, economic or other (response draws on instrument of national power)	• Green New Deal Violators are identified • Social Media providers challenged (Facebook, Google) • Non-compliant businesses and products come under attack via strike, boycott or other	• Grass-roots call for representation (DC, Puerto Rico, etc.) • Call for leadership change • Introduction of bills calling for sweeping change • Call to challenge current leadership • Call to re-brand party

BIBLIOGRAPHY

Aceves, W. J. (2018). Virtual Hatred: How Russia Tried to Start a Race War in the United States. *Mich. J. Race & L.*, *24*, 177.

Allen, T. S., & Moore, A. J. (2018). Victory without Casualties: Russia's Information Operations. *Parameters*, *48*(1), 59-71.

Barnett, R. W. (1998). Information operations, deterrence, and the use of force. *Naval War College Review*, *51*(2), 7-19.

Bennett, M., & Waltz, E. (1982). Counter deception principle and applications for National Security (Boston: Artech House, 2007), and earlier, Donald C Daniel and Katherine L. Herbig, eds., Strategic military deception.

Blight, J. G., & Welch, D. A. (1998). The Cuban missile crisis and intelligence performance. *Intelligence and National Security*, *13*(3), 173-217.

Boatwright, B. C., Linvill, D. L., & Warren, P. L. (2018). Troll factories: The internet research agency and state-sponsored agenda building. *Resource Centre on Media Freedom in Europe*.

Broersma, M., & Graham, T. (2012). Social media as beat: Tweets as a news source during the 2010 British and Dutch elections. *journalism practice*, *6*(3), 403-419.

Charters, D. (1985). Richard H. Shultz and Roy Godson, Dezinformatsia: Active Measures in Soviet Strategy.

CNN. (1998, January). Inside the KGB: An Interview with Retired KGB Maj. Gen. Oleg Kalugin. Retrieved from

https://web.archive.org/web/20070206020316/http:/www.cnn.com/SPECIALS/cold.war/episodes/21/interviews/kalugin/

Chen, A. (2015). The agency. *The New York Times*, *2*.

Coats, D. R. Director of National Intelligence, "Statement for the Record Worldwide Threat Assessment of the US Intelligence Community," Senate Select Committee on Intelligence, January 29, 2019.

DiResta, R., Shaffer, K., Ruppel, B., Sullivan, D., Matney, R., Fox, R., ... & Johnson, B. (2019). The tactics & tropes of the Internet Research Agency.

Elving, R. (2019, June 14). Fear of Foreign Interference in U.S. Elections Dates from Nation's Founding. Retrieved from https://www.npr.org/2019/06/14/732571895/fear-of-foreign-interference-in-u-s-elections-dates-from-nations-founding

Fursenko, A., & Naftali, T. (1998). Soviet intelligence and the Cuban missile crisis. *Intelligence and National Security*, *13*(3), 64-87.

Garthoff, R. L. (1998). US intelligence in the Cuban missile crisis. *Intelligence and National Security*, *13*(3), 18-63.

Giles, K. (2016). Handbook of Russian information warfare.

Giles, K., Sherr, J., & Seaboyer, A. (2018). Russian Reflexive Control.

Hansen, J. H. (2002). *Soviet deception in the Cuban missile crisis*. CENTRAL INTELLIGENCE AGENCY WASHINGTON DC CENTER FOR THE STUDY OF INTELLIGENCE.

Heuer Jr, R. J. (1981). Strategic deception and counterdeception: A cognitive process approach. *International Studies Quarterly*, *25*(2), 294-327.

Jervis, R. (2017). *Perception and misperception in international politics: New edition*. Princeton University Press.

Johnson, J. (2016, January 6). Statement by Secretary Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector. Retrieved from https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical

Kahneman, D., & Tversky, A. (1972). Subjective probability: A judgment of representativeness. *Cognitive psychology*, *3*(3), 430-454.

Kasapoglu, C. (2015). *Russia's Renewed Military Thinking: Non-linear Warfare and Reflexive Control*. NATO Defense College, Research Division.

Komar, D. M. (1995). *Information-Based Warfare: A Third Wave Perspective*. AIR WAR COLL MAXWELL AFB AL.

Marantz, A. (2019). *Antisocial: Online Extremists, Techno-Utopians, and the Hijacking of the American Conversation*. Viking.

Miller, C. C. (2010, April 9). Twitter Acquires Atebits, Maker of Tweetie. Retrieved from https://bits.blogs.nytimes.com/2010/04/09/twitter-acquires-atebits-maker-of-tweetie

Mueller, R. S. (2019). *The Mueller Report: Report on the Investigation into Russian Interference in the 2016 Presidential Election*. WSBLD.

Murthy, D. (2011). Twitter: Microphone for the masses? *Media, culture & society*, *33*(5), 779-789.

Palmer, A. (2019, August 21). Dozens of celebrities fall for Instagram hoax. Retrieved from https://www.cnbc.com/2019/08/21/instagram-denies-viral-terms-of-service-hoax-that-tricked-rick-perry-celebrities.html

Rayome, A. D. N. (2019, December 16). Facebook was the most-downloaded app of the decade. Retrieved from https://www.cnet.com/news/10-most-downloaded-apps-of-the-decade-facebook-dominated-2010-2019/

Roberts, J. Q. (2015). *Maskirovka 2.0: Hybrid Threat, Hybrid Response* (No. OP-Roberts-2015). Joint Special Operations University MacDill AFB United States.

Ribeiro, F. N., Saha, K., Babaei, M., Henrique, L., Messias, J., Benevenuto, F., ... & Redmiles, E. M. (2019, January). On microtargeting socially divisive ads: A case study of Russia-linked ad campaigns on Facebook. In *Proceedings of the Conference on Fairness, Accountability, and Transparency* (pp. 140-149).

Scales, R. H. (2009). Clausewitz and world war IV. *Military Psychology*, *21*(sup1), S23-S35.

Scaparrotti, C. (2012). *Joint doctrine for information operations* (No. JOINT-PUB-3-13). JOINT CHIEFS OF STAFF WASHINGTON DC.

Shelton, H. (1998). *Joint doctrine for information operations* (No. JOINT-PUB-3-13). JOINT CHIEFS OF STAFF WASHINGTON DC.

Thompson, J. R., Hopf-Wichel, R., & Geiselman, R. E. (1984). *The Cognitive Bases of Intelligence Analysis* (No. R83-039C). LOGICON INC WOODLAND HILLS CA OPERATING SYSTEMS DIV.

Tversky, A., & Kahneman, D. (1974). Judgment under uncertainty: Heuristics and biases. *science*, *185*(4157), 1124-1131.

Weedon, J., Nuland, W., & Stamos, A. (2017). Information operations and Facebook. *Retrieved from Facebook: https://fbnewsroomus. files. wordpress. com/2017/04/facebook-and-information-operations-v1. pdf*.

Wilson, C. (2007, March). Information operations, electronic warfare, and cyberwar: Capabilities and related policy issues. Library of Congress Washington DC Congressional Research Service.

Wohlstetter, R. (1962). *Pearl Harbor: warning and decision*. Stanford University Press.

ACADEMIC VITA
Calvin D. Mende

EDUCATION:

The Pennsylvania State University, University Park, PA *May 2020*
College of Information Science and Technology -
B.S. Security and Risk Analysis: Intelligence Analysis &
Data Modeling Focus
Minor: Information Sciences and Technology

EXPERIENCE:

Joint Interagency Task Force – South (JIATF-S) **Key West, FL**
Intelligence Assistant *May 2019-Aug 2019*

- Supported the Counter Drug and Counter Narcotic Mission
- Assisted senior intelligence staff in querying various intelligence databases in support of JIATF-S analytical products as well as national level requests.
- Conducted quality control and data management to ensure applicability and validity of sources and data
- Responsible for the accountability and review of intelligence collected by the Task Force, which resulted in the closure of 410 critical movement alerts and the tracking and accountability of 146.1 Metric Tons of Cocaine and 36,407 Pounds of Marijuana into the Consolidated Counterdrug Database (CCDB)

Pennsylvania State University, College of IST **University Park, PA**
Red Cell Lab Analyst *May 2017-Aug 2017, May 2018-Aug 2018*

- Organized the testing, training, integration, and briefing of NGA's emerging geospatial analytic tool called GeoQ
- Managed historic crime data of past city-wide events to enable geospatial hotspot analysis that allowed for effective law enforcement resource allocation during that year's upcoming event
- Briefed law enforcement on next possible target neighborhoods in an ongoing string of thefts from vehicles using Google and Esri geospatial suites
- Designed Epidemic Outbreak Simulation for Hershey Medical students to aid in decision making during high-stress
- Prepared a red team analysis of potential threats to Beaver Stadium in the wake of the Ariana Grande Concert, 2017
- Coordinated and collaborated with 10 other team members on projects in the field of Security and Risk & Analysis

Pennsylvania State University, College of IST **University Park, PA**
Learning Assistant *Aug 2018-May 2019, Aug 2019-May 2020*

- Following classes: Decision Making and Game Theory, Deception and Counter Deception, The Intel Environment, SRA Capstone
- Duties included grading assignments, locating academic integrity violations, and assisting with lectures
- Consulted with instructor to adapt curriculum in a way that encourages higher student participation

Academic Integrity Board, College of IST **University Park, PA**
Undergraduate Representative *Aug. 2018-May 2020*

- Convened multiple times to hear cases of student academic integrity violations within the college
- Discussed the facts and reasoning of each case with staff and faculty in order to produce a ruling on the violation

ACCOMPLISHMENTS **NCAA STUDENT ATHLETE**

Schreyer Honors College PSU
Dean's List - *Fall 2015 – May 2020*
Red Cell Analytics Lab Club Member

Big Ten Distinguished Scholar
Big Ten All-Academic
Athletic Director's Leadership Institute