2023-06

RUSSIAN DISINFORMATION CAMPAIGNS IN THE UNITED STATES AND POSSIBLE COUNTERMEASURES

Williams, Michael R.

Monterey, CA; Naval Postgraduate School

https://hdl.handle.net/10945/72292

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

RUSSIAN DISINFORMATION CAMPAIGNS IN THE UNITED STATES AND POSSIBLE COUNTERMEASURES

by

Michael R. Williams

June 2023

Thesis Advisor:	Neil C. Rowe
Second Reader:	Shannon C. Houck

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** June 2023	**3. REPORT TYPE AND DATES COVERED** Master’s thesis

4. TITLE AND SUBTITLE RUSSIAN DISINFORMATION CAMPAIGNS IN THE UNITED STATES AND POSSIBLE COUNTERMEASURES	**5. FUNDING NUMBERS**
6. AUTHOR(S) Michael R. Williams	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

This thesis investigates the complex realm of Russian disinformation, including its historical roots, its dissemination methods, and its possible countermeasures. Historical instances of disinformation, ranging from the Cold War era to contemporary times, suggest consistent themes, motives, and strategies employed by Russia in shaping narratives, manipulating public opinion, and undermining democratic processes. By examining social media, state-controlled media outlets, propaganda, and cyberoperations, we see an intricate web of techniques employed to disseminate false information, amplify divisive narratives, and exploit existing vulnerabilities in target societies. This thesis also examines possible countermeasures to combat Russian disinformation, and by drawing upon case studies and best practices, it analyzes the effectiveness of strategies such as fact checking, media-literacy programs, and international sharing of information. We also need to bolster cybersecurity, promote transparency in social media platforms, and develop comprehensive legislation to address the multifaceted nature of the disinformation challenge.

14. SUBJECT TERMS Russia, influence, disinformation	**15. NUMBER OF PAGES** 65
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

THIS PAGE INTENTIONALLY LEFT BLANK

RUSSIAN DISINFORMATION CAMPAIGNS IN THE UNITED STATES AND POSSIBLE COUNTERMEASURES

Michael R. Williams
Lieutenant, United States Navy
BS, Montana State University – Northern, 2002

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN CYBER SYSTEMS AND OPERATIONS

from the

NAVAL POSTGRADUATE SCHOOL
June 2023

Approved by: Neil C. Rowe
Advisor

Shannon C. Houck
Second Reader

Alex Bordetsky
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis investigates the complex realm of Russian disinformation, including its historical roots, its dissemination methods, and its possible countermeasures. Historical instances of disinformation, ranging from the Cold War era to contemporary times, suggest consistent themes, motives, and strategies employed by Russia in shaping narratives, manipulating public opinion, and undermining democratic processes. By examining social media, state-controlled media outlets, propaganda, and cyberoperations, we see an intricate web of techniques employed to disseminate false information, amplify divisive narratives, and exploit existing vulnerabilities in target societies. This thesis also examines possible countermeasures to combat Russian disinformation, and by drawing upon case studies and best practices, it analyzes the effectiveness of strategies such as fact checking, media-literacy programs, and international sharing of information. We also need to bolster cybersecurity, promote transparency in social media platforms, and develop comprehensive legislation to address the multifaceted nature of the disinformation challenge.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AMWG	Active Measure Working Group
CIA	Central Intelligence Agency
CNA	computer-network attacks
CND	computer-network defenses
CNE	computer-network exploitations
CNO	computer-network operations
EBLA	Eliminating Barriers to the Liberation of Africa
EU	European Union
EW	electronic warfare
IO	information operations
MILDEC	military deception
MISO	Military Information Support Operations
NATO	National Atlantic Treaty Organization
NF	National Front
NIST	National Institute of Standards and Technology
OPSEC	operations security
PSYOP	psychological operations
USCYBERCOM	United States Cyber Command

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I want to express my sincerest gratitude and appreciation to my thesis advisor, Dr. Neil Rowe, for his invaluable guidance and support throughout the process of writing this thesis. Dr. Rowe has been an exceptional mentor, providing insightful feedback and constructive criticism and motivating me to push myself further than I thought possible. His dedication and commitment to my success were evident in every meeting, and I am genuinely grateful for the time and effort he invested in me.

I would also like to thank my co-advisor, Dr. Shannon Houck. I am grateful for the time and effort she invested in reviewing and providing feedback on my drafts and her willingness to share her ideas and suggestions for improvement.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. OVERVIEW

As technology advances and the distribution of news and information becomes easier, manipulating news and information has become easier. This creates opportunities for national adversaries to gain an advantage. Over the last two decades, disinformation and misinformation have become so common in digital media that it can be difficult for readers to distinguish the truth. This includes both misinformation and disinformation (Merriam-Webster, n.d.). Misinformation is incorrect or misleading information, while disinformation is when deceptive information is intentionally spread to influence public opinion or hide the truth. Disinformation can be part of an "influence operation" for political or military goals.

Influence operations use disinformation to "weaponize" information against an enemy. They try to manipulate public opinion, disrupt activities, or destroy entities. The psychological effects of disinformation are fear, confusion, and cynicism. For example, in 2020, COVID-19 vaccine rumors and conspiracy theories ranged from "vaccines don't work" to more elaborate ideas like "the government is putting microchips in vaccines to track you" (Kelen & Maragakis, 2022). On social media such as Facebook and Twitter, some groups discouraged people from getting vaccinated, contributing to the spreading of the COVID-19 virus and many deaths. Disinformation can overwhelm its audience with dramatic fake statistics, fake correlations, and emotional stories. Users on social media that "like" and "share" this content with their followers help disperse these false stories. Healthcare professionals have complained that they not only have to fight the COVID-19 pandemic but also an "infodemic," which the World Health Organization defines as too much information, including false or misleading information during a disease outbreak (Eysenbach, 2020). Much like a virus, misinformation and disinformation can spread quickly.

Russia has run many online influence and disinformation campaigns targeting countries. Since at least 2013, the Russian government has used a unit called the Internet

Research Agency, whose primary mission is to spread “dezinformatsiya” or disinformation (Boghardt, 2009). Their disinformation campaigns are coordinated operations that contrive false, misleading, or manipulated information to destabilize their enemies. Technological advancements have greatly helped Russia’s campaigns (Martin et al., 2019). This thesis will examine how Russian influence campaigns have grown, their current methods, their effectiveness, and possible countermeasures.

B. BACKGROUND

In 1923 the Russian government created a “special disinformation office” to manage “false information with the intention to deceive public opinion (Prokhorov, 1973).” These campaigns have targeted race, ethics, and political issues, including elections, for 100 years. It was noted (Kennan, 1946):

> [They] undermine general political and strategic potential of major western powers. Efforts will be made in such countries to disrupt national self-confidence, to hamstring measures of national defense, to increase social and industrial unrest, to stimulate all forms of disunity ... [P]oor will be set against rich, black against white, young against old, newcomers against established resident, etc.

As an illustration, in 1982, an English newspaper in India published an article titled “Operation INFEKTION,” which said that the United States was responsible for creating and spreading the HIV/AIDS virus (Shevchenko, 2023). Since it was difficult to check the validity of such a claim, it created distrust and political division in the U.S. government. Furthermore, U.S. media only detected the Operation INFEKTION article six years later. Today, similar stories circulate on the Internet rapidly and reach millions of readers. Malicious software such as botnet technology, password crackers, and distributed denial of service (DDoS) are used by Russian cyber actors in these influence campaigns.

More recently, a report revealed Russia’s “bots” (automated Internet processes), “trolls” (online provocateurs), social media, impersonation, and other technical methods to disrupt democracy and interfere with the United States Presidential election (Mueller, 2019). However, Mueller’s criminal investigation was completed three years after the 2016

Presidential election, long after the damage was done, allowing Russia three years to improve its methods for future election meddling.

Much of this disinformation is offered by impersonators. Although social media platforms are trying to curtail or deter profile impersonators, large-scale remedies have yet to be implemented (Allcott et al., 2019). This is especially troubling given that nearly 55% of adult Americans receive daily news from social-media sources like Twitter, Facebook, Instagram, YouTube, Reddit, and Snapchat (Suciu, 2019). Also, legitimate online news sources can show disinformation when they have been victims of site defacement or unauthorized modification of their sites.

C. OUTLINE

This thesis will discuss how influence campaigns are constructed and implemented and how Russia uses them, identifying historical and current strategies. It will describe how technological advancements aid Russia's active measures and influence campaigns. It also suggests ways to discover and debunk Russian disinformation and the importance of media literacy.

This thesis has five chapters. Chapter II describes a historical perspective on disinformation campaigns, influence campaigns, and specific Russian influence campaigns, including 20th-century election meddling, post–Cold War strategies, and campaigns exploiting preexisting conflicts. Chapter III analyzes the technologies and social media platforms that Russia uses for disinformation and how they can be identified. Chapter IV suggests countermeasures and makes recommendations for combatting Russian disinformation campaigns. Chapter V gives a final assessment and suggestions for future work.

THIS PAGE INTENTIONALLY LEFT BLANK

II. HISTORICAL PERSPECTIVES ON DISINFORMATION CAMPAIGNS

A. INFORMATION OPERATIONS

The DOD defines Information Operations (IO) as a military activity involving a set of capabilities or tactics concerning information. DOD Joint Publication (JP) 3–13 says that information operations have five pillars: "computer-network operations (CNO), which include computer-network attacks (CNA), computer-network defenses (CND), and computer-network exploitations (CNE); psychological operations (PSYOP); electronic warfare (EW); operations security (OPSEC); and military deception (MILDEC)" (U.S. Joint Chiefs of Staff, 2012). When U.S. Cyber Command (USCYBERCOM) was established in 2010 as a unified combatant command, CNO became "cyberspace operations," including offense and defense (USCYBERCOM, 2010). Along with this change came its own doctrine (U.S. Joint Chiefs of Staff, 2022). Also, in 2010, PSYOP became "military information support operations" (MISO) to reflect PSYOP personnel deployed to U.S. embassies overseas (Myers, 2017).

How is information used to get people to believe or trust in a narrative beneficial to the teller? It helps to distinguish:

- Propaganda: An argument or story told to sway people's political or social ideas (U.S. Joint Chiefs of Staff, 2012). It is possible for it to be true while yet being deceptive, or it might be false. Propaganda is used when a government wants to increase the effectiveness of its efforts to communicate its goals, policies, and values through public affairs such as speeches and press releases (Cohen, 2021). For example, the Taliban used propaganda in Afghanistan to promote their ideology, recruit fighters, and undermine the Afghan government's and foreign forces' legitimacy (Walla, 2021). They used religious language and symbolism to appeal to people's religious beliefs and represented themselves as Afghanistan's only legitimate Islamic authority. They also used propaganda to criticize the Afghan government and foreign forces as "un-Islamic" and not respecting Islamic values. To recruit fighters, the Taliban represented themselves as a legitimate resistance movement fighting against a foreign occupation and corrupt government. They also used images of martyrs and fighters to appeal to young men disillusioned with Afghanistan's current political and social situation (Al Jazeera, 2022). They undermined the legitimacy of the Afghan government and foreign forces by portraying the Afghan government as corrupt and illegitimate and foreign forces as occupiers interfering in Afghan affairs (Jensen, 2021). They also criticized the Afghan government and foreign forces for their lack of progress in development, security, and governance.

- Misinformation: False information spread for entertainment or other purposes not intended to influence. False conspiracy theories or hoaxes have been disseminated through social media without concrete evidence (Cohen, 2021). Misinformation is common in social media. Because of the ease of distributing information, it is common to see misinformation shared, and many users do not check its validity (Allen, 2023).

- Disinformation: False information that is not propaganda. Examples are spreading fake news through media outlets and tampering with private or classified messages. Because disinformation is knowingly false information, it differs from misinformation by being more powerful and destructive. A recent example is when the Chinese government appeared to conduct an online disinformation campaign about COVID-19 that blamed the outbreak on the United States (Kurlantzick, 2020).

In an information-warfare campaign, accurate factual information rather than propaganda, misinformation, and disinformation can also help convey a clear and accurate message to the target audience. Factual information is information that can be independently verified and is based on objective evidence. Ensuring that the factual information used in a campaign is accurate, relevant, and up-to-date can be crucial. Misrepresenting or distorting the facts can undermine the campaign's credibility and damage the organization's reputation. Examples of factual information are:

- Statistics: Data such as the number of people affected by a problem, such as the prevalence of a particular disease or the economic impact of a specific policy (Turcilo & Obrenovic, 2020). Politicians often use statistics to justify their campaign claims or policy development. Statistics are also helpful in microtargeting voters, a marketing technique that uses data analytics and digital technology to identify and reach narrow groups of people with personalized messages or advertisements. It analyzes large amounts of data such as browsing history, online behavior, social media activity, and other demographic information (Patterson, 2018). Barack Obama's 2008 and 2012 presidential campaigns extensively used microtargeting (Issenberg, 2020). They used data analytics to identify supporters and donors and created targeted messages and advertisements to reach these groups.

- Expert opinions: Quotes and opinions from experts in relevant fields, such as medical professionals, academics, or industry leaders. It can give credibility to a campaign. Expert opinion from accredited doctors was used to combat the misinformation spread during the COVID-19 pandemic (Contreras, 2023).

- Historical facts: Information about the history of an issue or topic to provide context and help people understand the roots of a problem. An example is showing footage of past wars that honor the sacrifices made by military personnel throughout history. During the Vietnam War, the U.S. government referred to the shared heritage of the Vietnamese people and the Americans to gain public support.

- Scientific evidence: For campaigns related to health, the environment, or technology, scientific studies and research can support arguments and claims. During the Cold War, the U.S. and the Soviet Union advertised their technological advancements in nuclear weapons and space exploration to gain advantages in the arms race.

B. INFLUENCE

Possible tactics in influence operations include (Larson et al., 2009):

- Understand the target audience: Deep understanding of the target audience's beliefs, values, motivations, and decision-making enables tailored influence operations. In the military, this is used in recruiting. By understanding the demographics of people more likely to join the armed services, recruiters can spend more time in schools and communities that favor better results. For instance, recruits will likely come from families in the middle of the wealth distribution with a median wealth of $87,000 (Stickles, 2022).

- Build trust and credibility: Use credible sources, testimonials, and consistent messaging.

- Use obfuscation, confusion, and the disruption or diminution of truthful reporting and messaging. Russia has chosen this more contemporary propaganda model (Paul & Matthews, 2016). Russia appears to have enjoyed some success.

- Make emotional appeals: This can be achieved through images, stories, and symbols that resonate with the target audience. In the war between Russia and Ukraine, Russians have posted images of Russian soldiers and vehicles on the Internet since the Russian invasion of Ukraine began (Brody, 2022). Some of these showed the flag of the Soviet Union, apparently to appeal to Ukrainians that were sympathetic to the Soviet Union in the past.

- Use a multi-channel approach: Use a variety of traditional and digital media to reach a wider audience.

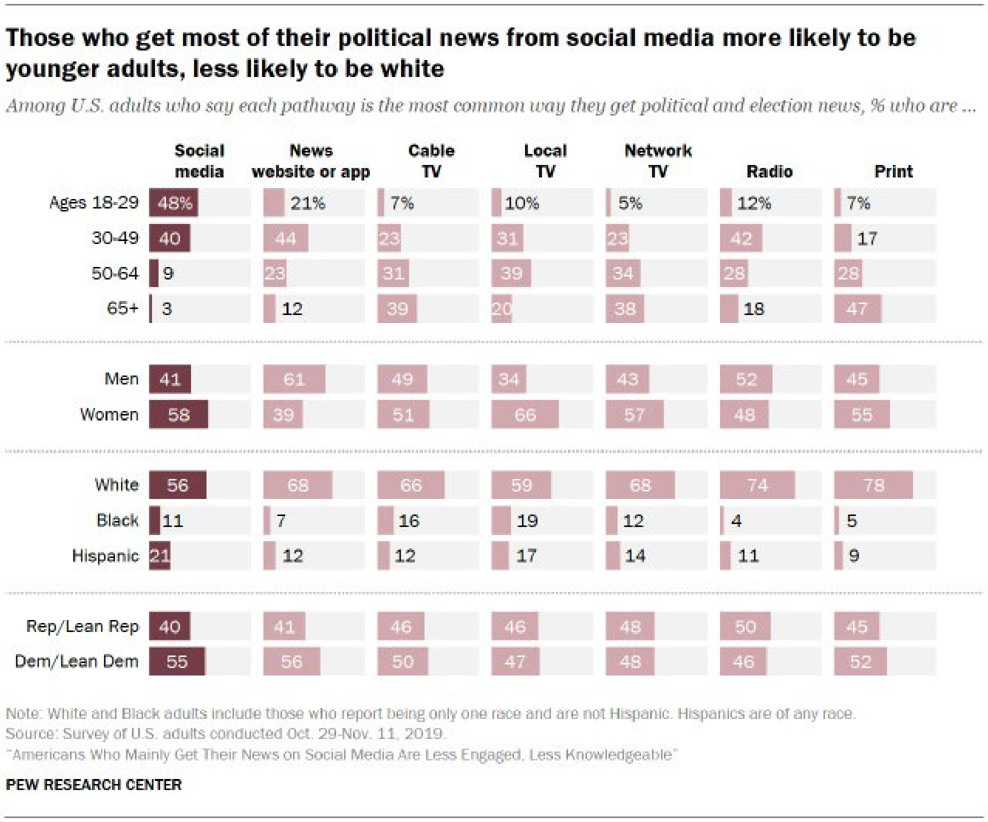
- Monitor and adapt continually: Since the effectiveness of an influence operation can change over time, one must adjust the operation to the evolving situation and feedback from the target audience.

- Encourage groupthink: This psychological phenomenon occurs within a group of people with strong cohesion and a desire for unanimity, leading them to make irrational or dysfunctional decisions in conformity to the group (Janis, 1972). Groupthink can lead to a narrow-minded mentality that stifles creativity, critical thinking, and dissenting opinions, resulting in suboptimal decisions.

C. INFLUENCE IN MARKETING

Influence is well understood in marketing, providing some models for political influence. It affects the success of a marketing campaign or strategy (Peek, 2023). Several external factors can affect success:

- Demographic factors: Age, gender, economic, occupation, status, and location of the people involved can be used to identify a target audience (Nadeem, 2020). For instance, in a study shown in Figure 1, a person in the age range of 18–29 is more likely to get their news from social media, and a person over the age of 65 is more likely to get their news from a print source (Nadeem, 2020). These demographics enable a political influence campaign to target subpopulations more effectively.



Those who get most of their political news from social media more likely to be younger adults, less likely to be white

Among U.S. adults who say each pathway is the most common way they get political and election news, % who are ...

Note: White and Black adults include those who report being only one race and are not Hispanic. Hispanics are of any race.
Source: Survey of U.S. adults conducted Oct. 29-Nov. 11, 2019.
"Americans Who Mainly Get Their News on Social Media Are Less Engaged, Less Knowledgeable"

PEW RESEARCH CENTER

Figure 1. Demographic factors. Source: Nadeem (2020).

- Technological factors: Social media, websites, and smartphone applications are examples of technology that can influence in different ways. Marketers can gather information about the behavior of their targets to assess the best marketing methods.

- Political factors: A country's political situation can affect its influence environment (Weir, 2019). The decisions made in politics can affect the regulations, tariffs, and other standards that control the expenses of buying products and carrying out operations. Also, politics can affect the global economy, altering a country's actions.

- Social factors: The attitudes and beliefs commonly held by a population include various aspects such as career, age, and social interactions (Nadeem, 2020). Multiple social factors influence the way people react to social experiences. An example is when a company donates money to charitable organizations to help those in need. One’s beliefs, opinions, and values may be influenced by the people that governments or organizations engage with and the values an organization portrays.

- Internal marketing influences: Several internal factors can affect marketing operations as well (Peek, 2023):
- Employees: Teams involved in marketing promote content and products while engaging with consumers.
- Managers: People in a company with leadership positions make decisions about services, products, and work processes. They may also develop campaigns and strategies for launching new products.
- Systems: An organization’s marketing and work processes rely on technology to reach their marketing objectives.
- Materials: A business’s inventory of the resources used in designing services or producing goods.

D. INFLUENCE OPERATIONS IN GUATEMALA

As an example of a political influence operation, the Central Intelligence Agency (CIA) played a significant role in Guatemala during the Cold War era. In 1954, it orchestrated a coup that overthrew democratically elected President Jacobo Árbenz, who had implemented land reforms that were thought a threat to the interests of the United States (Anglis, 2021). Influence operations contributed to the success of the coup. The operations involved propaganda, financial support for anti-government groups, and the arming and training rebel forces (Kane, 2019).

The CIA spread propaganda and disinformation through radio, television, and newspapers. They also produced pamphlets highlighting a supposed communist threat in Guatemala. In addition, the agency created a network of informants and agents within the Guatemalan government, military, and business community. By sowing fear and confusion among the population, the CIA conveyed a message that communism was the actual threat and cause of their troubles. Because of the CIA's support to overthrow the government using covert actions and psychological warfare, Árbenz resigned from office and fled to the Mexican embassy in Guatemala City.

E. RUSSIAN INFLUENCE CAMPAIGNS

Russia is experienced in electoral interference (Mueller, 2019). The CIA investigated Russian election interference in the 1964, 1968, and 1984 U.S. presidential elections (Jones, 2022). Largely unconcerned with political parties, the Russians generally encouraged votes for candidates that did not directly oppose communist politics and practices.

According to the CIA's pre-Soviet Union demise estimates, the Soviets were believed to have spent roughly $3 billion annually on disinformation campaigns. (McMahon, 1980). Propaganda efforts decreased in pace after the disintegration of the Soviet Union but continued to be well-coordinated and concentrated on promoting a communist regime in Russia (Abrams, 2016). For example, the Russians tried to sway Western public opinion by warning of the dangers that would follow the fall of the USSR (Schoen & Lamb, 2012). The U.S. Active Measure Working Group (AMWG) worked to debunk Russian disinformation attempts, and they succeeded for a time (USIA, 1992; Abrams, 2016).

To capitalize on confusion after the terrorist attack on September 11, 2001, the Russian media and television outlets of RT and Sputnik promoted conspiracy theories suggesting that the attack was coordinated by the United States (Hotchkiss, 2019). Despite the lack of evidence, they became headlines in U.S. newspapers. After 2001, Russia mainly targeted former Soviet states, the National Atlantic Treaty Organization (NATO), and the European Union (EU) (Topor & Tabachnik, 2021). Russian disinformation campaigns occurred against Europe, Sweden, Ukraine, Estonia, and others, and campaigns became bolder. For instance, when Russia shot down a Malaysian aircraft over Ukraine in 2014, Russian actors posted many reports that a Ukrainian fighter jet was responsible for the crash (Lewis & Marwick, 2017). However, an investigation later confirmed that a Russian surface-to-air-missile was responsible.

In the 2016 U.S. Presidential election, Russia found Donald Trump to be a favorable candidate. Disinformation increased on social media, promoting Trump and denigrating his primary competitor, Hillary Clinton. The anti-Clinton campaign used doctored photos and videos, such as those showing Clinton shaking hands with the Al Qaeda leader, which were widely distributed across social-networking sites (Jensen et al., 2019). Russian actors also used spear phishing against a Clinton campaign member, John Podesta, and accessed email correspondence between him and the presidential candidate. These were later released through Wikileaks, an anti-secrecy organization used in other Russian disinformation campaigns. Another disinformation campaign ("Pizzagate") alleged that a pizza parlor was a child sex-trafficking ring supervised by Hillary Clinton (Horton, 2020). Pizzagate escalated to the extent that a gunman drove 300 miles to free victims he believed to be trapped in the basement. It was circulated using botnets traced to St. Petersburg and was reposted by many people, including Donald Trump to his 36 million followers.

Russian disinformation often exploits tensions in a society. For example, between 2015 and 2017, a campaign using at least 13 accounts created over 129 Facebook events (O'Sullivan, 2018). 300,000 people viewed the event invitations, and 65,000 confirmed that they would attend the event. The activities were planned around various contentious political topics to turn people in the United States against one another. In one instance, they planned and publicized two events from opposite points of view and held them on the same day and in the same location in Houston, Texas, hoping to create violence. This disinformation campaign only cost $200 to coordinate but could have caused hundreds of thousands of dollars in personal and property damage (Allbright, 2017).

The Russian government's disinformation operations represent a significant threat to democratic societies. The Russian government employs various tactics, such as spreading false information, fabricating social media profiles, and promoting divisive content, in an attempt to create chaos, erode faith in democratic establishments, and ultimately achieve its geopolitical objectives (Jones, 2022). These tactics have effectively exploited societal fault lines and amplified existing divisions, with significant consequences for domestic politics and international relations. Addressing the challenge of Russian disinformation operations requires a coordinated effort from governments, civil society organizations, and technology companies.

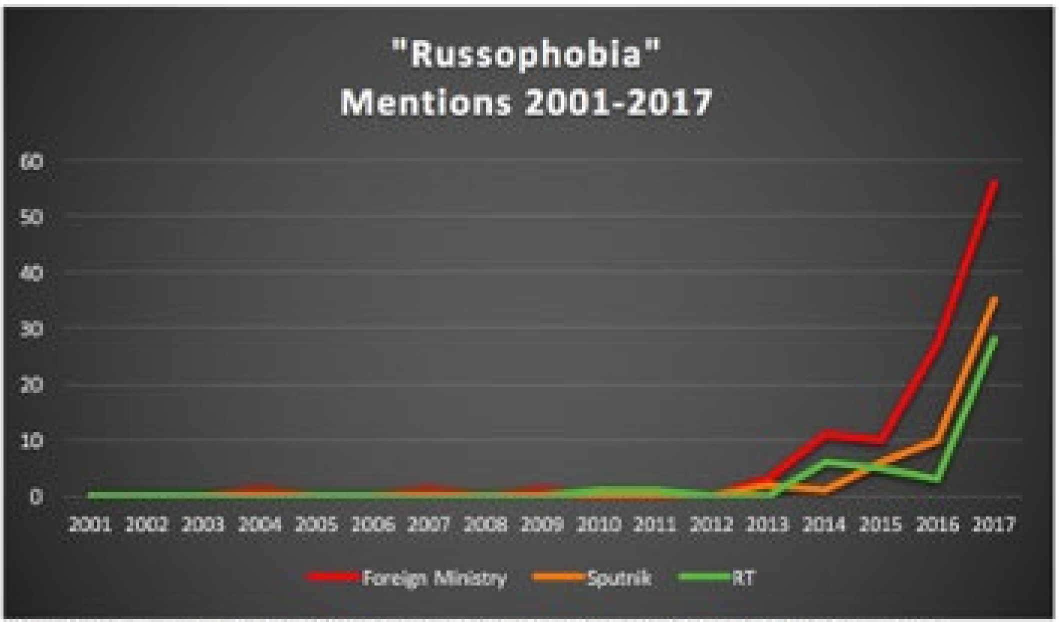
III. METHODS OF SPREADING DISINFORMATION

A. DISINFORMATION METHODS

Over the years, Russia has created a set of false narratives that it persistently injects into the global information environment through its disinformation and propaganda ecosystem (U.S. Department of State, 2022). These narratives are adjusted to fit circumstances. They often show little relation to truth, as they come from a country without a free press to contradict them and are solely designed to shape the information environment to support Russian policy goals. We identify five commonly heard narratives.

1. Theme 1: Russia Is the Victim

Russian authorities frequently depict their nation as a targeted party and rationalize their forceful actions as requisite reactions to the conduct of the United States and its associates (U.S. Department of State, 2022). The Russian government accuses the United States of engaging in "Russophobia" and labels anyone questioning Russian activities as xenophobic and Russophobic. This tactic was used significantly following the invasion of Ukraine in 2014 (Welle, 2021), for which Russia maintained that the international community reacted negatively to the invasion because people feared and despised Russia. The figure below shows that until Russia invaded Ukraine, the Russian Foreign Ministry and state-funded disinformation sources did not mention Russophobia (DFRLab, 2018).



Entries for Sputnik before 2014 refer to its predecessor, Voice of Russia

Figure 2. Graph displaying the terms "Russophobia" and "Russophobe" mentioned by RT, Sputnik, and the Russian Foreign Ministry between 2001 and 2017. Source: DFRLab (2018).

2. Theme 2: Historical Revisionism

Russian narratives often distort history to make Russia appear more favorably (U.S. State Department, 2022). This is done when history does not support Russia's political goals. As an example, the Soviet Union and Nazi Germany signed the Molotov-Ribbentrop non-aggression pact in 1939, which posed political challenges for the government. As a result, a misleading account of the start of World War II was presented. It has been observed that Russia tends to exaggerate by accusing individuals who do not share their distorted version of history as Nazis.

We see a similar narrative with the 2022 Russian invasion of Ukraine (Beauchamp, 2022). Early in the conflict, the Russian government denied involvement, and its news media claimed that the Ukrainian government was responsible for the unrest in eastern Ukraine. However, as the conflict escalated and Russian military personnel and equipment were clearly observed in the region, Russia represented itself as a protector of ethnic Russians in Ukraine and a defender of Ukraine's territorial integrity. According to Russia, Ukraine was taken over by Nazis, who intervened to rescue Ukraine. This was achieved through the annexation of Crimea and the support provided to separatists in eastern Ukraine.

3. Theme 3: The Collapse of Western Civilization is Imminent

Another narrative that is common in Russia is the idea that Western civilization is in decline and has forsaken “traditional values” because it defends the rights of LGBTQ+ people, supports gender equality, and encourages diversity favorably (U.S. State Department, 2022). Since the 19th century, Russians have referred to “the rotting West,” an idea that comes from Karl Marx (Kirchick, 2014). This story is told from a “values” perspective, and hence it uses words like “tradition,” “family values,” and “spirituality.” Russia asserts that it supports these values and gender norms and takes a stand against the “decadence” of the United States of America and other Western nations favorably (U.S. State Department, 2022). The Western world, according to Putin, has replaced the terms “mother” and “father” with “parent 1 and 2,” while Foreign Minister Lavrov has said that students in Western countries “learn at school that Jesus Christ was bisexual” (Times, 2023).

4. Theme 4: The U.S. Creates Revolutions Themselves

Russia has accused the United States of inciting revolutions in several countries, including Kazakhstan, Moldova, Georgia, Kyrgyz Republic, Ukraine, and countries in the Middle East and Africa favorably (U.S. State Department, 2022). Russia tends to challenge the legitimacy of popular movements that are pro-democracy, pro-reform, or not in their geopolitical interests. They often assert that the United States is secretly supporting these movements. (Cordesman, 2022). These charges are leveled against groups that are part of civil society as well as independent media outlets that report on violations of human rights and corruption. Russia frequently rejects the idea that the people of other nations have agency, dignity, and the right to speak for themselves independently.

5. Theme 5: The Kremlin Can Shape Reality According to Their Desires.

When reality is too far from the narrative it wants to give, Russia creates alternative realities and sows uncertainty about reality. Contradicting storylines can confuse targets and deter responses, which is done with state-funded misinformation sources and social media (Gamberini, 2020). For example, on March 4, 2018, Russia tried to kill former Russian military intelligence officer Sergei Skripal and his daughter Yulia. Within four weeks after that event, the Russian state-run media outlets RT and Sputnik spread 735 articles with 138 different and sometimes contradictory stories (U.S. Department of State, 2022). Russia has used this strategy to shift attention away from its participation in events such as the downing of Malaysia Airlines Flight 17 and the invasion and occupation of Georgia in 2008 (Demirjian, 2014).

B. RUSSIAN ACTORS

Russia uses many actors for disinformation, including both state actors formally linked with a government and non-state actors posing as enterprises or civil society (Klimburg, 2011). A good non-state actor is more appealing to a Russian misinformation campaign since it allows the government to deny involvement; examples are cyber terrorists, non-governmental groups, hackers, and hacktivists (Traynor, 2007). Hacktivists employ anonymous cyber proxies to participate in cyber civil disobedience for political causes; anyone can use a proxy for their Internet browser by following instructions on the Internet. Instructions for doing ICMP floods, TCP SYNC floods, and general ping floods for cyberattacks were provided in Russia to allow amateurs to participate in Estonian cyberattacks in 2007 (Saleem & Hassan, 2009). Another example is when Internet trolls targeted a Finnish journalist investigating Russian cybercrime (Aro, 2016). Internet bullies bombarded them with threats to their personal and professional reputations, intimidated interviewees, and waged Facebook and Twitter campaigns against them.

Russia has also used non-governmental organizations to propagate disinformation. Such organizations appear less biased, letting them participate in “soft” tasks like education, history, and cultural exchanges (Linvill & Warren, 2020). Non-governmental organizations can also better conceal their influences. The Ghanaian organization "Eliminating Barriers to the Liberation of Africa" (EBLA), which supported Internet activism and human rights, was, for example, closely linked to the Russian Internet Research Agency (Ward, 2020). EBLA's objectives included influencing the 2016 United States Presidential election by emphasizing persecution in black neighborhoods, police brutality, and civil rights problems. EBLA established Facebook and Twitter pages in Internet media read by predominantly black communities around the United States.

Russia creates disinformation through its agencies and employs civilians to produce media. The Internet Research Agency, a highly guarded structure known as the "Troll Factory" in St. Petersburg, Russia, manages this (Aro, 2016). Employees create and distribute the material on the Internet, and they operate like a factory with specialized sections to foster societal animosity and undermine political authority. The U.S. Justice Department charged Russian Internet Research Agency personnel in February 2018 for interfering with the 2016 presidential elections with trolls on social networking sites (The United States of America v. Internet Research Agency LLC, 2018).

C. MEDIA PLATFORMS IN DISINFORMATION CAMPAIGNS

False social-media information can travel faster than verified news since it can encourage its spread by design (Zannettou et al., 2018). Since any user can create a website, discussion board, or social media account, it is easy to report disinformation. Twitter, Facebook, and Instagram social-media platforms have been used by Russian disinformation campaigns (Woolley, 2016). Facebook, for instance, has 2.2 billion active users and offers easy signup by requiring only a name, email, and birthday. Furthermore, user identities are unverified, so malicious actors can create multiple accounts to share disinformation and are not required to mention Russia. To combat these efforts, Facebook reportedly deleted over three billion fake accounts in 2019 (Stengel, 2020), but this was after the 2016 election.

Twitter allows users up to 2400 posts daily (Vosoughi et al., 2017), which is ideal for a disinformation campaign. Humans cannot produce disinformation that fast, but bots can, and Twitter bots have become valuable to cyber criminals. Twitter says it denies over

500,000 new user requests from bots daily with CAPTCHA authorization, a weak form of verification (Twitter, 2020). "Cyborgs," human-assisted bots, have now bypassed authentication efforts effectively (Chu, 2012). Traditionally, the number of followers, likes, and reposts of a user reflect their popularity and influence, so bots try to generate large amounts of such activity to make themselves look credible and popular. Fake accounts are valuable for spreading disinformation because anonymity prevents accountability. Twitter auditing revealed in 2018 that nearly 60% of President Donald Trump's Twitter followers were bots (Fishkin, 2018). Following the 2016 election, Twitter published a list of over 10 million fake accounts and their posts to show the public the impact and reach of Russian disinformation (Twitter, 2020). However, researchers estimate that 15% of Twitter's user databases are still undetected bots (Varol et al., 2017).

Russia also spreads disinformation on cultural and subgroup message boards like 4chan and Reddit. 4chan is a site where users communicate anonymously with little moderation, and it contains much hate and extremist speech on topics such as white supremacy and anti-Semitism. In June 2020, white supremacists on 4chan launched a Twitter disinformation campaign to exacerbate racial tensions (Merrin, 2019). They tried to overwhelm popular Twitter hashtags like #BlackLivesMatter, #BLM, #AllWhitesAreNazis, and #AWAN with disinformation. These posts came from a small number of accounts and were posted simultaneously with similar content, so they were suspicious and should have been recognized by Twitter management. These were likely Russian trolls posing as both white supremacists and black activists.

Reddit is a discussion website with shared links, images, and dialog. Unlike 4chan, Reddit is controlled by moderators and is only semi-anonymous, which makes it harder for trolls to exploit. However, disinformation still gets posted. Reddit banned a popular subgroup posting disinformation about President Trump, "r/The_Donald," due to racism, sexism, bigotry, and falsified information (Hurtado et al., 2019).

The Russian government also broadcasts "official" disinformation through domestic media platforms such as Sputnik and Russia Today. These often criticize independent media institutions (Fernquist, Kaati, & Schroeder, 2018). Much of their disinformation is lies or half-truths about espionage, terrorism, and national elections.

D. ELECTION INTERFERENCE

1. The United States

Russia has been trying to influence elections worldwide since the 17th century (Shimer, 2020). Election interference is also a goal of many Russian military operations. Many of these disinformation campaigns aim to sow discord among the population and attempt to get elected the candidate that best suits Russia's interests.

In the 1964 U.S. presidential election between Lyndon Johnson and Barry Goldwater, the Soviet Union saw the conservative Goldwater as a threat (Jones, 2022). Moscow was very concerned about Goldwater's anti-Soviet beliefs, and Soviet and Czechoslovak intelligence agencies launched a disinformation operation portraying Goldwater as a racist and mentally unfit for office. Georgy Filatov, a researcher at the Russian Academy of Sciences, created a document that illustrates this objective (Shandra, 2021). The document was found in the Russian State Archive of Contemporary History, and it translates to:

> Top secret. Instance number two.
>
> For the Central Committee of The Communist Party of the Soviet Union.
>
> The Ministry of Foreign Affairs of the USSR and the KGB under the Council of Ministers of the USSR consider it expedient, in connection with the electoral campaign in the United States, to implement in the near future through closed channels of third countries a number of active measures (publication of materials in the foreign press we use, instigation in the relevant political circles of information, etc.) designed to have a beneficial effect on the foreign policy of the Soviet Union on the course and results of the presidential elections in the United States and to strengthen anti-Goldwater sentiments both in the United States itself and in other capitalist and neutralist countries.
>
> At the same time, it is understood that some of the planned measures, after their implementation, can be used by the U.S. Democratic Party and its press in their own interests in the preelection struggle against Goldwater.
>
> The main direction of the planned activities is to show:
>
> 1. Goldwater's victory in the elections and pursuit of the foreign policy course outlined in the program of the Republican Party would mean a

> decline in U.S. authority among both allied and neutralist states, leading to U.S. political isolation from Europe, Asia, Africa, and Latin America.
>
> 2. The possibility of Goldwater's election as president causes concern throughout the bourgeois world and is already a source of discord in NATO, since the U.S. allies, given Goldwater's extremism, cannot allow him to play with their fate, don't want to associate themselves with his program that threatens the outbreak of a nuclear war. Goldwater's rise to power would lead to intensify the confrontation between the United States and its allies.
>
> 3. The coming to power of Goldwater, openly proclaiming methods of interference in the affairs of other states, and primarily in the internal affairs of socialist countries, would have led to an aggravation of U.S. relations with these countries, and above all with the USSR, would have increased the danger of an atomic conflict.
>
> Along with this, the Ministry of Foreign Affairs of the USSR and the KGB under the USSR Council of Ministers consider it desirable to prepare and implement measures to discredit Goldwater as a person among the American population. This means, in particular:
>
> a) To prepare a document indicating the indirect involvement of Goldwater as a far-right leader in the assassination of President Kennedy. To propose, if necessary, to make this document public shortly before the election day to prevent Goldwater and his supporters from taking appropriate countermeasures.
>
> b) To inspire documented information abroad that Goldwater periodically suffers from mental disorders (maniac, drug addict).
>
> We ask for consent.
>
> Vasily Kuznetsov [First Deputy Minister of Foreign Affairs of the USSR]
>
> Chairman of the KGB under the Council of Ministers of the USSR Vladimir Semichastny.
>
> September 3, 1964

One "active measure" by the Soviets was creating and delivering printed disinformation materials in the United States and worldwide and sent to many journalists and politicians. The hope was that U.S. and foreign news organizations would propagate this disinformation material and spread it further. A former Czechoslovak intelligence official claimed. “I believe the outcome was far more successful in developing countries than in the United States (Jones, 2022).”

It is difficult to prove that the interference in the 1964 election by the USSR changed the outcome, but the intent was there. This same intent was seen in the 2016 U.S. presidential election. The investigation led by Special Counsel Robert Mueller looked into Russian efforts to manipulate the election, including possible collaboration between the Trump campaign and Russian actors and whether the campaign committed any financial crimes (Mueller et al., 2019). This report revealed the lengths Russia went to manipulate this election with planning years in advance. In 2014, Russian agents traveled to the U.S. to create social media accounts on various political issues (Parks, 2019). They amassed hundreds of thousands of likes and followers and earned credibility and reach by gaining retweets and interaction from Trump supporters and associates such as Kellyanne Conway and Donald Trump Jr. This let them reach a wider audience (Abrams, 2019). This groundwork was like that in marketing campaigns for understanding the audience.

Another key element of this election interference was Russian operatives stealing Hillary Clinton’s emails (Mueller et al., 2019). Because a foreign adversary hacked her, she lost some credibility as a leader. Also, her emails could be used as ammunition against her (Keith, 2016). When the margin of victory is small, swaying the vote a little with influence operations can be enough to change an outcome (O’Neill, 2022).

In the 2020 presidential election, Putin authorized “influence operations aimed at denigrating President Biden’s candidacy and the Democratic Party, supporting Trump, undermining public confidence in the electoral process and exacerbating socio-political divisions in the U.S.” (Intelligence Community Assessment, 2021). Russian agents used more fake social media accounts and attempted to hack into email servers and state voting systems. This time however, the U.S. government and social-media platforms were more aware of Russia’s tactics and stopped many attacks (Facebook.com, 2021) by locking down and actively monitoring servers (CISA, 2022). Efforts to reduce disinformation spread were also implemented by locating and removing thousands of fake accounts (Culliford, 2021). However, they could only remove a few since Facebook has 2.2 billion daily users and Instagram has over a billion (Bushwick, 2022). Social media platforms now use artificial intelligence to identify fake accounts and disinformation (Anand, 2022), but this task is also not simple. Another issue is whether social-media platforms are willing to remove this content of influence operations when it earns them money.

2. Election Interference in Other Countries

The U.S. is not alone as a victim of Russian election meddling (Brattberg & Maurer, 2018). In the 2017 Netherlands general elections, Dutch intelligence officials feared Russian interference like that during U.S. presidential elections might also happen to them. In January 2018, the Dutch Foreign Minister confirmed that the Dutch intelligence agency, AIVD, had provided information to the U.S. about Russian interference in the U.S. election of 2016. In March 2018, AIVD claimed that Russian hackers had tried to get into the Dutch government's systems. The report claimed the hackers were part of the Cozy Bear group associated with the Russian intelligence agency FSB. In January 2018, the Dutch intelligence agency and the police's cybercrime unit established a task force to monitor and prevent future foreign interference in elections.

The French also have seen election interference from the Russians. The French 2017 election saw hacking attempts and disinformation campaigns (Hosenball, 2017). In February 2017, the Macron campaign reported targeting by an extensive hacking attack that released thousands of emails and documents. Some text was altered to create false narratives about the campaign. Furthermore, Russian-based media outlets such as RT and Sputnik promoted anti-Macron propaganda and spread false information about the candidate. The French government tried to counter foreign interference by increasing cybersecurity and promoting media literacy and critical thinking. Although Macron won the election, the hacking and disinformation may have influenced voter opinions and contributed to a more polarized electorate.

In 2014, Ukraine faced a major political crisis when Russia invaded and annexed Crimea. Then there were claims of Russian interference in Ukraine's political affairs and presidential elections (Polityuk & Zinets, 2019). Russia was accused of conducting disinformation campaigns by spreading false information, spreading propaganda, and manipulating media narratives to undermine the legitimacy of Ukraine's government.

Russia was also alleged to have supported separatist movements in eastern Ukraine's Donetsk and Luhansk regions, which aimed to establish independent entities aligned with Russia. Cyberattacks were also directed at Ukraine during this period, with evidence pointing to Russian involvement (Joselow, 2016). These attacks targeted various government institutions, electoral infrastructure, and media outlets, apparently to disrupt Ukraine's political and electoral processes. Russia also supported pro-Russian candidates and parties in Ukraine; allegations of financial assistance, political backing, and attempts to manipulate election results to favor candidates sympathetic to Russia's interests were made.

The conflict between Russia and Georgia in 2008 showed Russian interference in another former Soviet Union republic. The situation was complex and multifaceted, involving military operations, political tensions, and territorial disputes. While election interference was not a significant part of the conflict, there were allegations of Russian involvement in Georgia's political processes then (Sanger & Santora, 2020).

Russia had close ties with the breakaway regions of Abkhazia and South Ossetia in Georgia, which had declared independence from Georgia in the early 1990s (Dickinson, 2021). Russia was accused of providing funding and political backing to these separatist movements, which played a significant role in the tensions leading up to the conflict. After the military conflict, Russia officially recognized the independence of Abkhazia and South Ossetia, despite the international community largely considering them as part of Georgia (Wolff, 2019). This move further complicated the political situation in the region and had implications for Georgia's sovereignty and territorial integrity.

Russia also sought to influence political dynamics in Georgia by supporting pro-Russian political parties and figures (Sanger & Santora, 2020). Georgia was also subject to cyberattacks during a conflict that disrupted its government and communication systems (Dickinson, 2021). The attacks were aimed at critical infrastructure, including government websites, news agencies, and banks. These cyberattacks are believed to be carried out by actors affiliated with Russia or Russia itself. Additionally, Russia was accused of spreading disinformation and propaganda to influence the narrative surrounding the conflict. This involved disseminating false information and misleading narratives through channels such as social media, news outlets, and online forums. The apparent goal was to create confusion, manipulate public opinion, and damage Georgia’s credibility. For instance, false information was also disseminated to portray Georgia as the aggressor in the conflict.

IV. COUNTERMEASURES AND RECOMMENDATIONS

Russian influence campaigns are complex and multifaceted, and countering them requires a comprehensive and multi-pronged approach (Bodine-Baron, 2018). Russia conducts influence campaigns differently depending on the target. If the target is a United States election, they try to divide conservatives and liberals; if the target is neighboring states, they try to divide ethnic Russian populations from their governments (Helmus et al., 2018). Knowing the target and how the Russians plan to attack it enables countermeasures with the best chances of success. monitoring elections

France had already been on alert in 2017 following allegations of Russian interference in the U.S. presidential elections in 2016 (Conley & Vilmer, 2022). It took some measures to counter meddling in elections. Nonetheless, the campaign of Emmanuel Macron was targeted on May 5, 2017, by a cyberattack that released thousands of emails and documents. This was just two days before the final round of presidential elections. The attack was later attributed to the group Fancy Bear, believed to be affiliated with Russian intelligence agencies. The group is known to use hacking to target political campaigns, government agencies, and other high-value targets. The cyberattack on Macron's campaign involved phishing emails that targeted campaign staff with malware-infected attachments. The attackers accessed the campaign's email system, allowing them to monitor communications and steal sensitive data.

After this attack, the French government established a task force called the National Coordination of the Protection of the Electoral Process (CNPPUE) (Daniels, 2017). It gathered representatives from government agencies, including the General Directorate for External Security, the agency responsible for conducting counterintelligence operations. The CNPPUE monitored social media and other online platforms for signs of disinformation and other attempts to influence the election (Conley & Vilmer, 2022). They also worked closely with political parties and candidates to improve online security and provided training on detecting and preventing disinformation campaigns. The government increased funding for cyber defense and established a cybersecurity center for the presidential campaign, staffed by experts from government agencies.

Russia may have provided financial support to Marine Le Pen and her party, the National Front (FN), during the 2017 French presidential election (Sonne, 2018). Evidence is a €9 million loan reportedly provided to the party by a Russian bank, the First Czech Russian Bank, in 2014. At the time, the FN was struggling financially, and this loan was seen as a lifeline for the party. However, Marine Le Pen has denied that this loan was linked to the 2017 election, and the Russian bank has since been shut down due to money-laundering allegations.

By good planning to counter foreign interference in their 2017 presidential election, France conducted their elections without significant interruption by outside influence campaigns. While releasing stolen data just before the second round of the election may have been embarrassing, it was not damaging (Daniels, 2017). The attack ultimately failed to sway the election, and Macron went on to win by a significant margin.

A. EDUCATING THE PUBLIC

A good way to counter Russian influence campaigns is to educate the public about their tactics, motivations, and goals (Matthews, 2021). While this can be effective, it is also hard to implement because of confirmation bias. This is a cognitive bias that means people tend to look at new information in a way that supports what they already believe (Simkus, 2023). The tendency is to look for, understand, and remember information to support one’s beliefs while dismissing or downplaying information against them.

Confirmation bias can cause people to read ambiguous information in support of what they already think, which can cause them to mistake or misinterpret the information. This can be especially hard when judging evidence or making choices based on information that needs to be completed or clarified. Confirmation bias can be especially strong with issues important to people’s identities or deeply held beliefs, like political or religious beliefs. People may reject information that goes against their beliefs.

Russian influence operations frequently exploit confirmation bias because targeted messaging and propaganda to reinforce preexisting beliefs and tendencies is a powerful persuasion method (Eckel, 2022). With sophisticated algorithms and machine learning, they can identify their target audience’s preferences, values, and beliefs and tailor their messaging to those biases. This can create a reinforcing loop in which people see information confirming their beliefs, making them more receptive to further propaganda and disinformation.

For critical thinking and making good decisions, one must be aware of confirmation bias. One must also consider how the same information can be seen and interpreted differently. This can help people identify disinformation and propaganda and reduce their campaigns' effectiveness (Ciampaglia, 2018).

To create a better-informed public, policymakers must provide ways to educate the public (Abrams, 2021). If they can see the long-term costs of having the public fall prey to disinformation campaigns, they may be more apt to promote educating the public on such matters. While a disinformation campaign conducted by an outside government might help a political campaign today, that might not always be the case in the future, and preventing disinformation from spreading is critical to a lasting democracy.

Other strategies to educate the public about influence campaigns are:

- Develop educational materials about disinformation campaigns: These can explain the tactics used, such as false information, misleading headlines, manipulation of images or videos, fake social-media accounts, and bots and trolls (Simkus, 2023). Educational materials can be distributed through social media, news outlets, and schools.

- Run public-awareness initiatives through social media, public events, and advertising. Civil society organizations, such as think tanks and advocacy groups, can help by conducting research.

- Public figures must be knowledgeable about identifying and countering disinformation campaigns (Abrams, 2021). Lawmakers y can create laws and regulations to prevent the spread of false information and limit the impact of disinformation campaigns.

- Encourage social-media companies to promote media literacy by informing users about identifying fake news, propaganda, and disinformation (Simkus, 2023). They can also label or remove content that appears to be disinformation by setting policies.

- Tracing and attributing disinformation to its sources: Network monitoring can analyze network traffic to identify patterns and trends that may indicate disinformation.

- Estimating influence can be done by causal inference (Smith et al., 2018). This involves identifying the causal effect of an event on an outcome of interest based on the relationships between users and their actions in a social-media network. This model accounts for both direct and indirect effects of users on each other and confounding factors that may affect the relationship between users and their actions. With this model, one can rank users based on their influence on the network to identify influential users more efficiently.

- Another method used for network monitoring is machine learning and natural-language processing to analyze Twitter data and identify clusters of users who spread false information (Huber, 2020). Network analysis can then identify the key influencers in these clusters. Researchers found that many disinformation campaigns were highly organized and coordinated, with a small group of key influencers driving the spread of false information.

- Once an influence campaign has been identified, attributing it to a source by forensic analysis of the network traffic is the next step (NIST, 2022). One method is to use the geolocation data found in the images' metadata on social media posts and emails. Another is to do an IP address analysis to locate servers used for distributing such information since they are often located near the source.

- If malware is associated with disinformation, its origins can be traced independently. The malware's code can be examined to identify distinctive characteristics or signatures that may help determine its source. Signatures can also be used in tracing network traffic. Signature identification can exploit information collected by antivirus vendors and security researchers on a more global scale (Smith et al., 2018).

B. PROMOTING MEDIA LITERACY

A more general solution to the challenge of disinformation is the improvement of media literacy, the accessing, analyzing, evaluating, and creating media in various forms (Guess et al., 2020). Literate users are more discerning consumers of information and better able to identify and critically evaluate sources of information. Media literacy involves understanding how media works, including how news is reported, how images and videos are created and edited, and how messages are conveyed through different media channels (Terrell, 2022). By understanding the consequences of sharing false or misleading information, people can become more cautious about what they share online and more likely to verify the accuracy of information before sharing it.

The related term “digital readiness” refers to a person’s or a community’s proficiency in using digital technologies, including Internet accessibility, digital devices, and digital literacy (Guess et al., 2020). It is the necessary knowledge, skills, and outlook to navigate and use digital technologies. People and societies lacking digital readiness may be more vulnerable to disinformation because they may lack the critical thinking skills to understand how information is created and disseminated and to effectively identify false or misleading information. For example, people unfamiliar with digital platforms or social media may not recognize when an online post has been manipulated or is part of a coordinated disinformation campaign (Terrell, 2022). Also, societies without digital readiness may have more robust digital infrastructure, making them more vulnerable to cyberattacks, hacking, and other forms of digital interference.

A study examined digital readiness gaps among American adults based on socioeconomic status, educational attainment, and age (Horrigan, 2020). It found significant disparities in digital readiness, with lower-income, less-educated, and older adults being less ready. It suggests that efforts to close these gaps should include increasing access to affordable Internet services and providing digital skills training and support.

C. INCREASING TRANSPARENCY

Another way to combat disinformation is for governments and social media to mandate increased transparency in political advertising by requiring disclosure of the sources of funding for political ads (Brennen & Perault, 2022), including the names of donors and the amounts donated. Social media and online advertising should also maintain archives of political ads that include this information (Horrigan, 2020). Fact-checking organizations can help verify the accuracy of political ads and identify misleading or false claims. On Internet pages, links to fact-checking results can be added automatically.

Supporting independent media can help promote transparency and provide diverse viewpoints to reduce disinformation's influence (Jozwiak, 2023). For instance, Radio Free Europe/Radio Liberty counters Russian influence campaigns by providing independent news and information where the government censors or heavily controls the media. It can help in these ways:

- Fact-based reporting: This can provide audiences with accurate information and counter disinformation campaigns (Sullivan, 2022).

- Investigative journalism: Investigations into corruption and human rights abuses where the media is suppressed (Jozwiak, 2023).

- Language expertise: News and information in local languages can counter-propaganda.

- Partnership with local media: Provide training and support for independent journalism (Sullivan, 2022) to strengthen the media in countries where it is suppressed.

D. STRENGTHENING CYBERSECURITY

To prevent hacking and other forms of cyberattacks used to aid the dissemination of disinformation, we must strengthen cybersecurity measures for political campaigns, government agencies, and critical infrastructure (Schneier, 2017). Firewalls, intrusion-detection systems, and antivirus software can significantly reduce unauthorized access to systems and networks. This can help prevent the creation of fake accounts that disinformation campaigns use to spread through compromised systems. Governments and political organizations can invest in more robust cybersecurity defenses, including encryption and multi-factor authentication, to control access better. Organizations can provide cybersecurity training to help employees recognize and respond to phishing attempts, malware, and other cyberattacks.

Regular security assessments can identify vulnerabilities in systems and networks and fix them before they can be exploited (Cavelty & Wenger, 2020). Improved information sharing between government agencies, political organizations, and technology companies can help to detect and respond to cyber threats more quickly and effectively. International cooperation between governments can reduce political interference by sharing information, coordinating responses, and imposing consequences for malicious cyber activity.

E. FACT CHECKING

The U.S. Constitution First Amendment guarantees a right to freedom of speech and expression, including the ability to share false information. Nonetheless, the Supreme Court has ruled that the Constitution does not protect certain types of speech, such as defamation, perjury, fraudulent schemes for financial gain, false light tort, and lies that cause significant emotional harm (Volokh, 2022). It can be challenging and expensive to refute false claims legally. Even if one successfully proves that the allegations are unlawful, the lies and disinformation may have already spread to the public and can be challenging to contain. Nevertheless, s independent fact-checking organizations that debunk false claims and provide accurate information can encourage people to verify the information before accepting it as true (Murray, 2016). Social media platforms can also help by providing mechanisms for users to report false or misleading content. When multiple reports are received, the posts can be reviewed and potentially removed if found to violate platform policies. Social media platforms can further refine their algorithms to prioritize content from reliable sources and deprioritize potentially misleading or false information. These measures can go a long way in limiting the reach and impact of false claims.

F. HOLDING ACCOUNTABLE THOSE RESPONSIBLE

When evidence of foreign political interference is found, those responsible should face the consequences (Eckel, 2022). Failure to acknowledge that crimes have been committed legitimizes criminal behavior. For instance, after the 2016 U.S. presidential elections, actions were taken against Russia (Lucas, 2020):

- The U.S. government imposed economic sanctions on Russian entities and people involved in the interference, including the IRA, which was identified as responsible for the social-media disinformation campaign.
- The Justice Department indicted 13 Russian nationals and three Russian companies associated with the IRA.
- The U.S. government expelled 60 Russian diplomats in 2018 and closed a Russian consulate.
- The news coverage increased public awareness about election interference, and the revelation of the tactics used by the Russians should reduce future interference.

V. CONCLUSIONS

Russian disinformation poses increasingly significant challenges to global stability, democratic processes, and information integrity. This thesis has explored the origins, strategies, and impacts of Russian disinformation campaigns, identifying the sophisticated tactics employed by Russian state actors to manipulate public opinion, sow divisions, and undermine trust in democratic institutions. From social-media manipulation to creating fake news outlets and weaponizing hacked information, Russia has shown significant adaptability in exploiting information vulnerabilities.

To combat this threat, a multi-faceted approach is essential. First, monitoring elections is crucial to safeguarding democratic processes. Establishing independent oversight bodies and deploying software tools can help detect and counter disinformation efforts. While the U.S. did bolster its monitoring and cybersecurity for the 2020 elections, it needs to continue this activity consistently. Russian disinformation campaigns will continue to evolve and adapt to new technology, and it is crucial to stay ahead of their tactics and techniques to counter them effectively.

International cooperation is essential in addressing the transnational nature of Russian disinformation campaigns. Governments, intelligence agencies, and civil society organizations must collaborate to share intelligence, exchange best practices, and develop coordinated responses. Multilateral forums and initiatives can facilitate information sharing, joint exercises, and policy harmonization to strengthen the fight against disinformation.

Technological advancements can also help detect and counter disinformation. Improved algorithms, machine-learning models, and artificial intelligence can help identify and flag deceptive content, aiding more accurate and reliable information. Collaboration between technology companies, researchers, and governments is necessary to develop and implement innovative solutions.

Exploring the psychological and cognitive factors that make individuals susceptible to disinformation helps design effective countermeasures. Research should explore the psychological mechanisms underlying the reception and spread of disinformation and identify good strategies for debunking false narratives. Research should also assess the effectiveness of media-literacy programs, fact-checking organizations, transparency measures, regulatory frameworks, and international partnerships. Comparative studies and careful evaluations can identify best practices and inform evidence-based policymaking.

LIST OF REFERENCES

Abrams, A. (2019, April 18). Here's what we know so far about Russia's 2016 meddling. *Time*. https://time.com/5565991/russia-influence-2016-election/

Abrams, Z. (2021). Controlling the spread of misinformation. https://www.apa.org/monitor/2021/03/controlling-misinformation

Al Jazeera (2022, February 22). Taliban to create Afghanistan 'grand army' with old regime troops. https://www.aljazeera.com/news/2022/2/22/taliban-create-grand-army-afghanistan-old-regime-troops

Allen, J. (2023, March 14). Misinformation amplification analysis and tracking dashboard — Integrity Institute. Integrity Institute. https://integrityinstitute.org/blog/misinformation-amplification-tracking-dashboard

Anand, A. (2022, November 3). Fake account detection using AI in Facebook. www.analyticssteps.com. https://www.analyticssteps.com/blogs/fake-account-detection-using-ai-facebook

Anderson, J., & Rainie, L. (2022, September 15). The future of truth and misinformation Online. Pew Research Center: Internet, Science & Tech. https://www.pewresearch.org/internet/2017/10/19/the-future-of-truth-and-misinformation-online/

Anglis, J. (2021, April 6). Operation PBSuccess: How the CIA overthrew Guatemala's democracy. All that's interesting. https://allthatsinteresting.com/operation-pbsuccess

Aro, J. (2016). The cyberspace war: Propaganda and trolling as warfare tools. *European view*, *15*(1), 121–132.

Atske, S. (2021, February 22). Misinformation and competing views of reality abounded throughout 2020. Pew Research Center's Journalism Project. https://www.pewresearch.org/journalism/2021/02/22/misinformation-and-competing-views-of-reality-abounded-throughout-2020/

Beauchamp, Z. (2022, February 24). Why is Russia invading Ukraine? Putin's "Nazi" rhetoric reveals his terrifying war aims. Vox. https://www.vox.com/2022/2/24/22948944/putin-ukraine-nazi-russia-speech-declare-war

Bodine-Baron, E. (2018, November 1). Countering Russian social media influence. RAND. https://www.rand.org/pubs/research_reports/RR2740.html

Boghardt, T. (2009). Soviet Bloc intelligence and its AIDS disinformation campaign. *Studies in Intelligence*, *53*(4): 1–24.

Brattberg, E., & Maurer, T. (2018). Russian election interference: Europe's counter to fake news and cyber attacks. *Carnegie Endowment for International Peace*. https://carnegieendowment.org/files/CP_333_Brattberg_Maurer_Russia_Elections_Interference_Brief_FINAL.pdf

Brennen, J. S. B., & Perault, M. (2022, March 9). How to increase transparency for political ads on social media. *Brookings*. https://www.brookings.edu/blog/techtank/2021/03/19/how-to-increase-transparency-for-political-ads-on-social-media/

Brisson-Boivin, K. (2021, April 14). How digital literacy can help close the digital divide. Policy Options. https://policyoptions.irpp.org/magazines/april-2021/how-digital-literacy-can-help-close-the-digital-divide/

Brody, P. (2022, March 11). Ukraine: Russian troops flying Soviet flag, symbol of 're-establishing Russian domination'. *The Observers – France 24*. https://observers.france24.com/en/europe/20220311-ukraine-ussr-soviet-flag-russia-troops

Bushwick, S. (2022, March 8). Russia's information war is being waged on social media platforms. *Scientific American*. https://www.scientificamerican.com/article/russia-is-having-less-success-at-spreading-social-media-disinformation/

Cavelty, M. D., & Wenger, A. (2020). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy*, *41*(1), 5–32. https://doi.org/10.1080/13523260.2019.1678855

Chu, Z., S. Wang, H. G., and Jajodia, S. (2012). Detecting automation of Twitter accounts: Are you a human, Bot, or Cyborg? In *IEEE Transactions on Dependable and Secure Computing*, *9*(6), pp. 811–824, Nov.–Dec. 2012.

Ciampaglia, G. L. (2018, June 21). Biases make people vulnerable to misinformation spread by social media. *Scientific American*. https://www.scientificamerican.com/article/biases-make-people-vulnerable-to-misinformation-spread-by-social-media/

CISA. (2022). Election infrastructure subsector – Specific plan: 2022 status update. *Cybersecurity & Infrastructure Security Agency*. https://www.cisa.gov/sites/default/files/publications/ei-ssp-2022-status-update_508.pdf

Cohen, R. S. (2021, July 19). Combating foreign disinformation on social media: study overview and conclusions. RAND report. https://www.rand.org/pubs/research_reports/RR4373z1.html

Conley, H. A., & Vilmer, J. J. (2022). Successfully countering Russian electoral interference. https://www.csis.org/analysis/successfully-countering-russian-electoral-interference#:~:text=The%202017%20French%20presidential%20election,nor%20in%20antagonizing%20French%20society.

Contreras, G. (2023, February 27). How an infectious disease expert interprets conflicting reports on COVID-19's origins. NPR. https://www.npr.org/2023/02/27/1159821909/how-an-infectious-disease-expert-assessed-how-covid-19-started

Cordesman, A. H. (2022, September 21). Russia and the "Color Revolution." https://www.csis.org/analysis/russia-and-color-revolution

Council, Y. E. (2019, January 28). Six easy ways to gain tremendous credibility for your company. *Forbes*. https://www.forbes.com/sites/theyec/2019/01/28/six-easy-ways-to-gain-tremendous-credibility-for-your-company/?sh=758d9c0060ff

Culliford, E. (2021, August 11). Facebook removes Russian network that targeted influencers to peddle anti-vax messages. Reuters. https://www.reuters.com/technology/facebook-removes-russian-network-that-targeted-influencers-peddle-anti-vax-2021-08-10/

Cybersecurity and Infrastructure Security Agency [CISA]. (2022, November 4). Election security rumor vs. reality. https://www.cisa.gov/rumor-vs-reality

Daniels, L. (2017, May 6). How Russia hacked the French election. *POLITICO*. https://www.politico.eu/article/france-election-2017-russia-hacked-cyberattacks/

Dawson, A., & Innes, M. (2019). How Russia's Internet Research Agency built its disinformation campaign. *The Political Quarterly*, *90*(2), 245–256. https://doi.org/10.1111/1467-923x.12690

Demirjian, K. (2014, July 22). Russia has many conspiracy theories surrounding Flight 17 crash. One involves long-dead people. *Washington Post.* https://www.washingtonpost.com/world/russians-have-many-theories-about-the-mh17-crash-one-involves-fake-dead-people/2014/07/22/9a1c5ec9-11b6-4384-b585-53fff62e5779_story.html

DFRLab (2018, July 10). #PutinAtWar: How Russia weaponized "Russophobia" – DFRLab – Medium. Medium. https://medium.com/dfrlab/putinatwar-how-russia-weaponized-russophobia-40a3723d26d4

Dickinson, P. (2021). The 2008 Russo-Georgian War: Putin's green light. Atlantic Council. https://www.atlanticcouncil.org/blogs/ukrainealert/the-2008-russo-georgian-war-putins-green-light/

Eady, G., Paskhalis, T., Zilinsky, J., Bonneau, R., Nagler, J., & Tucker, J. A. (2023). Exposure to the Russian Internet Research Agency foreign influence campaign on Twitter in the 2016 U.S. election and its relationship to attitudes and voting behavior. *Nature Communications*, *14*(1). https://doi.org/10.1038/s41467-022-35576-9

Eckel, M. (2022, December 8). Five things to know about the U.S. intelligence report on Russian election interference. *Radio Free Europe/Radio Liberty*. https://www.rferl.org/a/five-things-us-intelligence-report-russian-election-interference/31156225.html

Eysenbach, G. (2020). How to fight an infodemic: The four pillars of infodemic management. *Journal of Medical Internet Research*, *22*(6), e21820. https://doi.org/10.2196/21820

Facebook.com (2021, March 24). Removing more coordinated inauthentic behavior from Russia. Meta.com. https://about.fb.com/news/2019/10/removing-more-coordinated-inauthentic-behavior-from-russia/

Fernquist, J., Kaati, L., & Schroeder, R. (2018). Political bots and the Swedish general election. In *2018 IEEE International Conference on Intelligence and Security Informatics (ISI)* (pp. 124–129). Institute of Electrical and Electronics Engineers

Fishkin, R. (2018). We analyzed every Twitter account following Donald Trump: 61% are bots, spam, inactive, or propaganda. SparkToro. https://sparktoro.com/blog/we-analyzed-every-twitter-account-following-donald-trump-61-are-bots-spam-inactive-or-propaganda/

Gamberini, S. J. (2020, November 19). Social media weaponization: The biohazard of Russian disinformation campaigns. Center for the Study of Weapons of Mass Destruction. https://wmdcenter.ndu.edu/Publications/Publication-View/Article/2422660/social-media-weaponization-the-biohazard-of-russian-disinformation-campaigns/

Geiger, A. (2021, April 9). Political polarization in the American public. Pew Research Center – U.S. Politics & Policy. https://www.pewresearch.org/politics/2014/06/12/political-polarization-in-the-american-public/

Grisé, M. (2022, August 18). Rivalry in the information sphere: Russian conceptions of information confrontation. RAND. https://www.rand.org/pubs/research_reports/RRA198-8.html

Guess, A. M., Lerner, M. M., Lyons, B. A., Montgomery, J. M., Nyhan, B., Reifler, J., & Sircar, N. (2020). A digital media literacy intervention increases discernment between mainstream and false news in the United States and India. *Proceedings of the National Academy of Sciences of the United States of America*, *117*(27), 15536–15545. https://doi.org/10.1073/pnas.1920498117

Helmus, T. C. (2018, April 12). Russian social media influence: Understanding Russian propaganda in Eastern Europe. RAND report. https://www.rand.org/pubs/research_reports/RR2237.html#:~:text=Highlight%20and%20%22block%22%20Russian%20propaganda%20%28RP%29.%20Build%20the,better%20identify%20fake%20news%20and%20other%20propagandist%20content.

Horrigan, J. B. (2020, May 30). Digital readiness gaps. *Pew Research Center: Internet, Science & Tech*. https://www.pewresearch.org/internet/2016/09/20/digital-readiness-gaps/

Horton, A. (2020, March 30). After truth: How ordinary people are "radicalized" by fake news. *The Guardian*. https://www.theguardian.com/tv-and-radio/2020/mar/19/after-truth-hbo-fake-news-pizzagate-documentary

Hosenball, M. & Menn, J.(2017, April 21). Experts say automated accounts sharing fake news ahead of French election. *Reuters.com*. https://www.reuters.com/article/us-france-election-socialmedia-idUSKBN17M31G

Hotchkiss, M. B. (2019). Russian information warfare and 9/11 conspiracism: When fake news meets false prophecy. In *Developments in Information Security and Cybernetic Wars* (pp. 236–266). IGI Global.

Huber, B. R. (2020, July 21). Tracking misinformation campaigns in real-time is possible. Princeton School of Public and International Affairs. https://spia.princeton.edu/news/tracking-misinformation-campaigns-real-time-possible-study-shows

Hurtado, S., Ray, P., & Marculescu, R. (2019, April). Bot detection in Reddit political discussion. In *Proceedings of the Fourth International Workshop on Social Sensing* (pp. 30–35).

Intelligence Community Assessment. (2021). Foreign threats to the 2020 U.S. this federal elections (ICA 2020–00078D). www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf

Issenberg, S. (2020, April 2). How Obama's team used big data to rally voters. *MIT Technology Review.* https://www.technologyreview.com/2012/12/19/114510/how-obamas-team-used-big-data-to-rally-voters/

Janis, I. L. (1972). *Victims of groupthink: A psychological study of foreign-policy decisions and fiascoes*. Houghton Mifflin.

Jensen, B. (2021, August 16). How the Taliban did it: Inside the 'operational art' of its military victory. Atlantic Council. https://www.atlanticcouncil.org/blogs/new-atlanticist/how-the-taliban-did-it-inside-the-operational-art-of-its-military-victory/

Jones, S. G. (2022). Russian meddling in the United States: The historical context of the Mueller report. https://www.csis.org/analysis/russian-meddling-united-states-historical-context-mueller-report?fbclid=IwAR00UP-3tyqB-N9PlYKeNGqhpS1J6W-8DbS-CgQ3EE4P7EBn3VDxaDomDtw

Joselow, G. (2016, November 3). Election Cyberattacks: Pro-Russia hackers have been accused in past [Video]. NBC News. https://www.nbcnews.com/mach/technology/election-cyberattacks-pro-russia-hackers-have-been-accused-past-n673246

Jozwiak, R. (2023, April 3). Wider Europe briefing: Ukraine's big plan to fight Russian disinformation and why the EU is stalling on Belarus sanctions. *RadioFreeEurope/RadioLiberty*. https://www.rferl.org/a/wider-europe-jozwiak-ukraine-disinformation-belarus-sanctions/32346741.html

Kane, R. (2019, January 21). Operation PBSUCCESS: U.S. covert action in Guatemala – military strategy magazine. *Military Strategy Magazine*. https://www.militarystrategymagazine.com/article/operation-pbsuccess-u-s-covert-action-in-guatemala/

Keith, T. (2016, October 26). WikiLeaks reveals Clinton aides knew they had an email problem on their hands. NPR. https://www.npr.org/2016/10/26/499493544/wikileaks-reveals-clinton-aides-knew-they-had-an-email-problem-on-their-hands

Kelen, G. D., & Maragakis, L. (2022, April 29). *COVID-19 vaccines: Myth versus fact*. Johns Hopkins Medicine. https://www.hopkinsmedicine.org/health/conditions-and-diseases/coronavirus/covid-19-vaccines-myth-versus-fact

Kennan, G. (1946). George Kennan's "Long Telegram. *Wilson Center Digital Archive*. wilsoncenter.org. https://digitalarchive.wilsoncenter.org/document/george-kennans-long-telegram

King's College London (2019, March 1). Russian state media weaponizes news to sow confusion and division. https://www.kcl.ac.uk/news/how-russian-state-media-weaponises-news

Kirchick, J. (2014, January 3). Why Putin's defense of "Traditional Values" is really a war on freedom. Foreign Policy. https://foreignpolicy.com/2014/01/03/why-putins-defense-of-traditional-values-is-really-a-war-on-freedom/

Klimburg, A. (2011, January). Mobilising cyber power. *Survival*, vol. 53, no. 1, Taylor and Francis, pp. 41–60. https://doi.org/10.1080/00396338.2011.555595.

Kramer, A. E. (2021, September 20). How Russian officials "manage" elections with deceitful tactics. *New York Times*. https://www.nytimes.com/2021/09/17/world/europe/russia-elections-interference.html

Kurlantzick, J. (2020, September 10). How China ramped up disinformation efforts during the pandemic. Council on Foreign Relations. https://www.cfr.org/in-brief/how-china-ramped-disinformation-efforts-during-pandemic

Larson, E. B., Darilek, R. E., Gibran, D., Nichiporuk, B., Richardson, A., Schwartz, L. M., & Thurston, C. Q. (2009). Foundations of effective influence operations. A framework for enhancing Army capabilities. *PsycEXTRA Dataset*. https://doi.org/10.1037/e596982009-001

Lewis, B., & Marwick, A. (2017, May 15). Media Manipulation and Disinformation Online. Retrieved August 12, 2020, from https://datasociety.net/library/media-manipulation-and-disinfo-online

Linvill, D. L., & Warren, P. B. (2020). Troll factories: Manufacturing specialized disinformation on Twitter. *Political Communication*, *37*(4), 447–467. https://doi.org/10.1080/10584609.2020.1718257

Lucas, R. (2020, August 18). Senate releases final report on Russia's interference in 2016 election. NPR. https://www.npr.org/2020/08/18/903616315/senate-releases-final-report-on-russias-interference-in-2016-election

Matthews, M. (2021, August 16). *Understanding and defending against Russia's malign and subversive information efforts in Europe*. RAND. https://www.rand.org/pubs/research_reports/RR3160.html

McMahon, J. (1980). Soviet covert action (The Forgery Offensive). https://cryptome.org/cia-FM30-31B.htm#McMahon

Merriam-Webster. (n.d.). Definitions. In Merriam-Webster Dictionary. https://www.merriam-webster.com/dictionary

Merrin, W. (2019) President troll: Trump, 4Chan and memetic warfare. In: Happer C., Hoskins A., Merrin W. (eds) Trump's media war. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-319-94069-4_13

Miller, M. (2020, September 24). Facebook removes hundreds of accounts linked to Russian agencies ahead of election. The Hill. https://thehill.com/policy/technology/518113-facebook-removes-hundreds-of-accounts-linked-to-russian-agencies-ahead-of/

Mueller, R. (2019). *The Mueller Report: Report on the investigation into Russian interference in the 2016 Presidential Election*. Melville House.

Murray, B. A. (2016, November 22). How to report fake news to social media. BBC News. https://www.bbc.com/news/38053324

Myers, A. (2021, October 25). The best way to counter fake news is to limit person-to-person spread, Stanford study finds. https://news.stanford.edu/press-releases/2021/10/25/foil-fake-news-fs-infectiousness/

Myers, M. (2017, November 6). The Army's psychological operations community is getting its name back. *Army Times*. https://www.armytimes.com/news/your-army/2017/11/06/the-armys-psychological-operations-community-is-getting-its-name-back/

Nadeem, R. (2020, August 26). Demographics of Americans who get most of their political news from social media. *Pew Research Center's Journalism Project*. https://www.pewresearch.org/journalism/2020/07/30/demographics-of-americans-who-get-most-of-their-political-news-from-social-media/

NIST (2022). NIST publishes review of digital forensic methods.https://www.nist.gov/news-events/news/2022/05/nist-publishes-review-digital-forensic-methods

O'Neill, A. (2022, June 21). *Winning margins in U.S. elections 1789–2020 | Statista*. Statista. https://www.statista.com/statistics/1035992/winning-margins-us-presidential-elections-since-1789/

O'Sullivan, D. (2018, January 26). Russian trolls created Facebook events seen by more than 300,000 users. CNNMoney. https://money.cnn.com/2018/01/26/media/russia-trolls-facebook-events/index.html

Parks, M. (2019, April 18). Mueller's report shows all the ways Russia interfered in 2016 presidential election. NPR. https://www.npr.org/2019/04/18/714810702/muellers-report-shows-all-the-ways-russia-interfered-in-2016-presidential-electi

Patterson, D. (2018, November 7). How campaigns use big data tools to micro-target voters. CBS News. https://www.cbsnews.com/news/election-campaigns-big-data-analytics/

Paul, C., & Matthews, M. (2016). *The Russian "Firehose of Falsehood" propaganda model: Why it might work and options to counter it*. RAND Corporation eBooks. https://doi.org/10.7249/pe198

Peek, S. (2023, February 21). The science of persuasion: How to influence consumer choice. *Business News Daily*. https://www.businessnewsdaily.com/10151-how-to-influence-consumer-decisions.html

Polityuk, P., & Zinets, N. (2019, February 21). Ukraine security service accuses Russia of meddling in election. Reuters.com. https://www.reuters.com/article/us-ukraine-election-russia/ukraine-security-service-accuses-russia-of-meddling-in-election-idUSKCN1QA1OW

Prokhorov, A. M. (1973). Great Soviet encyclopedia. In *Macmillan eBooks* (Issue 1). http://fipak.areeo.ac.ir/site/catalogue/18324969

Saleem, M. & Hassan, J. (2009). *"Cyber warfare," the truth in a real case*. Project report, Linköping Universitetet, Sweden.

Sanger, D. E., & Santora, M. (2020, February 21). U.S. and allies blame Russia for cyberattack on Republic of Georgia. *New York Times*. https://www.nytimes.com/2020/02/20/world/europe/georgia-cyberattack-russia.html?auth=register-google

Schneier, B. (2017, November). *Cybersecurity campaign playbook*. Belfer Center for Science and International Affairs. https://www.belfercenter.org/publication/cybersecurity-campaign-playbook

Schoen, F., & Lamb, C. A. (2012). Deception, disinformation, and strategic communications: How one interagency group made a major difference. *Institute for National Strategic Studies*, *11*, 5. http://inss.ndu.edu/Portals/68/Documents/stratperspective/inss/Strategic-Perspectives-11.pdf

Shandra, A. (2021, December 26). How the USSR interfered in the 1964 U.S. presidential election: KGB memo. *Euromaidan Press*. https://euromaidanpress.com/2021/08/09/how-the-ussr-interfered-in-the-1964-us-presidential-election-kgb-memo/

Shevchenko, N. (2023). How the KGB convinced the world that AIDS was a Pentagon invention. *Russia Beyond*. https://www.rbth.com/history/333296-kgb-aids-operation-infektion-pentagon

Shimer, D. (2020). *Rigged: America, Russia, and one hundred years of covert electoral interference*. Knopf.

Simkus, J. (2023). Confirmation bias: Examples & observations. *Simply Psychology*. https://www.simplypsychology.org/confirmation-bias.html

Smith, S. T., Kao, E. K., Shah, D. C., Simek, O., & Rubin, D. B. (2018, June 1). Influence estimation on social media networks using causal inference. IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/8450823

Sonne, P. (2018, December 27). A Russian bank gave Marine Le Pen's party a loan. Then weird things began happening. *Washington Post*. https://www.washingtonpost.com/world/national-security/a-russian-bank-gave-marine-le-pens-party-a-loan-then-weird-things-began-happening/2018/12/27/960c7906-d320-11e8-a275-81c671a50422_story.html

Stengel, R. (2020). *Information Wars: How we lost the global battle against disinformation and what we can do about it*. Grove Press.

Stickles, B. (2022, March 9). How the U.S. military became the exception to America's wage stagnation problem. Brookings. https://www.brookings.edu/blog/order-from-chaos/2018/11/29/how-the-u-s-military-became-the-exception-to-americas-wage-stagnation-problem/

Suciu, P. (2019, October 11). More Americans are getting their news from social media. *Forbes*. https://www.forbes.com/sites/petersuciu/2019/10/11/more-americans-are-getting-their-news-from-social-media/?sh=2577f993e179

Sullivan, M. (2022, March 27). The Kremlin tries to stifle Radio Free Europe — And its audience surges. *Washington Post*. https://www.washingtonpost.com/media/2022/03/27/radio-free-europe-russia-ukraine/

Terrell.com (2022). 50 challenging activities to promote digital media literacy in students. *TeachThought*. https://www.teachthought.com/literacy/digital-media-literacy/

Times, M. (2023, March 16). Western schools teach children that Jesus was bisexual, Russian Foreign Minister says. *The Moscow Times*. https://www.themoscowtimes.com/2021/06/29/western-schools-teach-children-that-jesus-was-bisexual-russian-foreign-minister-says-a74365

Topor, L., & Tabachnik, A. (2021, December 1). Russian cyber information warfare. Marine Corps University. https://www.usmcu.edu/Outreach/Marine-Corps-University-Press/MCU-Journal/JAMS-vol-12-no-1/Russian-Cyber-Information-Warfare/

Traynor, I. (2007). Russia accused of unleashing cyberwar to disable Estonia. *The Guardian*, May 16, 2007.

Turcilo, L., & Obrenovic, M. (2020). Misinformation, disinformation, malinformation: Causes, trends, and their influence on democracy. *Heinrich Boll Stiftung*. https://www.academia.edu/44506424/Misinformation_Disinformation_Malinformation_Causes_Trends_and_Their_Influence_on_Democracy

Twitter (2020, June 12). Disclosing networks of state-linked information operations we’ve removed. Retrieved April 19, 2021, from https://blog.twitter.com/en_us/topics/company/2020/information-operations-june-2020.html

U.S. Department of State (2022, January 21). Russia’s top five persistent disinformation narratives – United States Department of State. https://www.state.gov/russias-top-five-persistent-disinformation-narratives/’

U.S. Joint Chiefs of Staff. (2022). Joint Publication 3-12: *Cyberspace Operations*. *https://irp.fas.org*. https://irp.fas.org/doddir/dod/jp3_12.pdf

U.S. Joint Chiefs of Staff. (2012). Joint Publication 3-13: *Information Operations*. *https://irp.fas.org*. https://irp.fas.org/doddir/dod/jp3_13.pdf

Volokh, E. (2022, October 19). *When are lies constitutionally protected?* Knight First Amendment Institute. https://knightcolumbia.org/content/when-are-lies-constitutionally-protected#:~:text=Punishable%20Lies,distress%20are %20all%20constitutionally%20unprotected.

Walla, K. (2021, August 26). Before the Taliban took Afghanistan, it took the internet. Atlantic Council. https://www.atlanticcouncil.org/blogs/new-atlanticist/before-the-taliban-took-afghanistan-it-took-the-internet/

Ward, C. (2020, April 11). How Russian meddling is back before 2020 vote. CNN. Retrieved June 4, 2020, from www.cnn.com/2020/03/12/world/russia-ghana-troll-farms-2020-ward/index.html.

Weir, K. (2019). Politics is personal. *American Psychological Association*. https://www.apa.org/monitor/2019/11/cover-politics

Welle, D. (2021, May 9). Putin: Russia will "firmly" defend interests. https://www.dw.com/en/victory-day-putin-says-russia-will-firmly-defend-interests/a-57474684

Whittaker, Z. (n.d.). Mueller report sheds new light on how the Russians hacked the DNC. techcrunch.com. Retrieved June 1, 2022, from https://techcrunch.com/ 2019/04/18/mueller-clinton-arizona-hack

Wike, R., Fetterolf, J., Fagan, M., & Moncus, J. J. (2022, April 6). Seven-in-ten Americans now see Russia as an enemy. Pew Research Center's Global Attitudes Project. https://www.pewresearch.org/global/2022/04/06/seven-in-ten-americans-now-see-russia-as-an-enemy/

Wolff, S. (2019). Georgia: Abkhazia and South Ossetia. *The Princeton Encyclopedia of Self-Determination*. https://pesd.princeton.edu/node/706

Woolley, S. C. (2016). Automating power: Social bot interference in global politics. *First Monday, 21*(4), 4th ser. doi:10.5210/fm.v21i4.6161

Zannettou, S., Caulfield, T., De Cristofaro, E., Sirivianos, M., Stringhini, G., & Blackburn, J. (2018). *Disinformation warfare: Understanding state-sponsored trolls on Twitter and their influence on the web*. https://dl.acm.org/doi /10.1145/3308560.3316495

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California