REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
29 March 2021	Master of Military Studies (MMS) thesis	AY 2020-2021

4. TITLE AND SUBTITLE

Protecting Americans from Russian Influence: Navigating the Polarity of Freedom of Speech and Security of Information

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
Goulet, Laura E. (MAJ)

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
USMC Command and Staff College
Marine Corps University
2076 South Street
Quantico, VA 22134-5068

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
N/A

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The resurgence of a Russian Cold War tactic of spreading disinformation through social media threatens to tip the balance of a polarity between freedom and security. Analysis of Section 230 of the Communications Decency Act of 1996 provides valuable insight into the complexities of the issues for US political leaders and private social media elites tackling foreign threats against US interests on social media platforms. This paper examines three policy alternatives to address the threat of Russian influence operations (IO) online. The results reflect that a joint private and public collaboration can best achieve the strategic objectives in the detection, defense and deterrence of Russian disinformation online, and expanding the Global Engagement Center under the US Department of State was the strongest solution to balance the freedom-security polarity.

15. SUBJECT TERMS

Russian Disinformation; Influence Operations; IO, Polarity of Freedom and Security; Section 230 of the Communications Decency Act of 1996

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			USMC Command and Staff College
Unclass	Unclass	Unclass	UU	38	19b. TELEPHONE NUMBER *(Include area code)* (703) 784-3330 (Admin Office)

United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

Protecting Americans from Russian Influence: Navigating the Polarity of the Freedom of Speech and Security of Information

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

Major Laura E. Goulet
March 29, 2021

AY 2020-21

—

MMS Mentor Team and Oral Defense Committee Member:
DR. RICHARD H. GRIMMETT
Approved: [signature]
Date: 19 APR 21

MMS Mentor Team and Oral Defense Committee Member:
Curtis A. Lineweaver
Approved: [signature]
Date: 19 APR 21

United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

Protecting Americans from Russian Influence: Navigating the Polarity of Freedom of Speech and Security of Information

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

Major Laura E. Goulet
March 29, 2021

AY 2020-21

—

MMS Mentor Team and Oral Defense Committee Member:
_____
Approved: _____
Date: _____

MMS Mentor Team and Oral Defense Committee Member:
_____
Approved: _____
Date: _____

Table of Contents

Acknowledgements:

My sincere appreciation to my advisor, Dr. Richard Hegmann, for his assistance in developing this thesis, and to Mr. Curtis Lineweaver for the continuous support in my research in Russian disinformation.

Executive Summary

The rapid rise of social media platforms predicated on empowering freedom of speech has provided foreign great power adversaries new avenues of attack against the United States. These platforms have moved beyond connecting distant family and friends and have become a tool for state and non-state actors to mask the advancement of their interests. The Russian Federation has weaponized social media platforms by spreading disinformation to the point where Americans can no longer discern the truth. Currently, Section 230 of the 1996 Common Decency Act protects private social media companies from liability for the content posted by their users. The overall intent of this clause is to prevent censorship and preserve the right to freedom of speech on the internet. Yet, with this constraint, the US Government (USG) and private social media companies are unable to adequately address the spread of disinformation. Russians and other competitors will continue to amplify domestic issues to sow discord in the country and delegitimize government institutions in an attempt to hurt the image of the US as a global leader and to undermine the political foundations of US power. Analysis of Section 230 provides valuable insight into the complexities of the issues for US political leaders and private social media elites tackling foreign threats against US interests on social media platforms.

The Russian use of disinformation against Americans during the 2016 presidential election was a clarion call for a solution. The resurgence of a Russian Cold War tactic of spreading disinformation now through social media threatens to tip the balance of a polarity between freedom and security. More broadly, viewing Russian activities through the lens of international relations explanations of great power competition, can prompt a reexamination of how traditional frameworks can be applied to novel domains and dominance of the information environment. The US Government must implement an adequate policy solution to establish a

multi-layer, security in depth approach in order to protect the information on which voters rely and strengthen American confidence in democratic institutions.

This paper examines three policy alternatives to address the threat of Russian influence operations (IO) while managing the existing polarity between freedom and security. The first alternative is to maintain the status quo; second, amend Section 230 of the 1996 Common Decency Act and hold tech companies more liable; and third, expand the Global Engagement Center under the Department of State. Each alternative was measured against criteria important to the interests of each key stakeholder such as performance, time, risk, feasibility, and cost. The results revealed that the expansion of the GEC was the strongest solution to balance the freedom-security polarity.

This paper argues that a joint private and public collaboration can best achieve the strategic objectives in the detection, defense and deterrence of Russian disinformation online. The main element to each of these security measures is information sharing among the public and private sector and educating the public. This approach acknowledges there are no easy solutions by optimizing mitigation efforts through a whole-of-nation approach while maintaining the balance of freedom and security.

DISCLAIMER

Introduction

During the 2016 presidential elections, the Russian Federation executed a widespread series of influence operations (IO) on social media platforms against the American electorate to sow discord and undermine American's confidence in US elections and democratic institutions. The goal of spreading disinformation on already hyper-partisan issues was to push Americans to vote for a candidate that Moscow perceived did not have a foreign policy strategy that interfered with Russian interests. As a result of the level of interference, the US government (USG) and private industry leaders scrambled to understand the elusive nature of the threat, causing "political paralysis" which in turn prevented an adequate response to protect the American electorate.[1]

The attack on the national electoral process incited national security concerns over Russian's ability to weaponize information and shape world order. It exposed how the very tools that enable free speech also allowed Russia to spread disinformation, in turn resurfacing the US domestic debate on legislation that protects social media companies from liability for the content posted on their websites. The Russian use of social media therefore presents a polarity for the United States Government (USG) and an emerging issue at the intersection of domestic politics and international relations that political and security professionals will need to examine continuously for years to come.[2] Russia's interference in the elections was the most "politically consequential information attack in history" that caused American's to doubt political leaders and the information shared with the public.[3] Though several changes were made by both the public and private sectors in preparation for the 2020 presidential elections, investigations of the

causes of the January 6 insurrection on the Capitol Building are looking for signs of any residual effects from the Russian influence in 2016.

This case study raises a number of emerging questions for researchers, of which likely the most important two are: how does Russia employ influence operations to interfere in US elections?, and what strategic approach and specific action does the USG need to take in order to protect the political legitimacy of national elections? This particular polarity highlights the need for a whole-of-nation response, but the USG must take the lead in building political legitimacy of national elections. How can the USG, responsible for protecting the security of American citizens, act in ways that maintain the privacy and free speech of these same citizens? The USG must implement an adequate policy solution to establish a multi-layer, security in depth approach in order to protect the information on which voters rely and strengthen American confidence in democratic institutions.

The purpose of this paper is to recommend a policy solution to help manage the interplay between freedom of speech and security for the American electorate. Using the case study of the 2016 Presidential Election, this paper will provide a background of the issue; provide a look into what Russian IO is; introduce key stakeholders; and examine three policy solutions. This study measures each proposed solution against five criteria significant to the stakeholders, and then proposes a final recommendation and implementation plan that will yield an achievable course of action. The intent of the proposed policy solution is to build a security measure that leaves American's more resilient to foreign information manipulation.

Background

The dynamics of social media and the use of influence operations have far outpaced any legislation governing online content and have created problems in balancing security and

freedoms for Americans. The 2016 elections uncovered the ways in which Russians are exploiting vulnerabilities as a result of the USG's mismanagement of the two. Responding to Russian influence operations is not new to the US, but the reemergence of the cold war tactic of disinformation on social media is still unfamiliar territory. Continuing to apply old Cold War frameworks to these tactics in a new domain with the domestic legal constraints such as Section 230 will not work.

The USG has been reluctant to impose regulations on the internet since it first attempted to restrict indecent content to minors through the Communications Decency Act (CDA) of 1996. The act was the first legislation attempt to regulate online activity which gave rise to debates on First Amendment rights on the internet, but the Supreme Court eventually deemed the act as unconstitutional. However, one piece of the act approved, Section 230, provided immunity for websites considered publishers and therefore responsible for content posted by their users.[4] The tech industry coined Section 230 as "the most important law in tech," but left the USG or citizens unable to legally hold Facebook or similar websites accountable for Russia's activity during the 2016 elections, or, for that matter, or any online content published by third parties.[5]

Advocates for Section 230 argue that without it, freedom of speech could be in jeopardy, paving the way for censorship by both web owners and the government. The very topic of Section 230 and the Common Decency Act is itself a parallel polarity, and there are many who, on either side of the political aisle, strongly oppose Section 230 or argue for it. It serves as another crossroad between freedom of speech and security. The hoped-for rationale [of Section 230]—that "if they received general immunity, they would be freer to remove antisocial content that violated their [own] terms of service"[6]—did not pan out in reality. Instead, freedom of speech online proliferated hate speech, harassment, bullying and eventually, a platform for

foreign and domestic terrorist recruiting. Social media companies have only taken just enough measures to remove harmful content to avoid government pressure. Michael Beckerman of the Internet Association argues against Section 230 as "not a blanket amnesty but a call for responsible policing of platforms."[7] As new threats surfaced during the 2016 and 2020 elections, the scope, scale and reach of issues the internet presented in 1996 versus 2016 and then in 2020 were largely different. The nature of the growing threat points to the need to revisit the protections the law provides to social media companies.

Companies like Facebook and Twitter predicated their platforms on philosophies that supported social justice and freedom of rights. They largely stayed away from politics until Congress and growing public opinion blamed them for the fallout from the 2016 election. After investigations revealed Russian activity and the illegal purchasing of political ads on its platform, Facebook acknowledged the risk that freedom of speech presented and has taken action to combat the spread of false information on its websites. Facebook hired 20,000 employees to focus on security and content review.[8] Artificial Intelligence (AI), previously applied towards fighting child pornography and anti-terrorism would now help identify patterns of disinformation. However, for every measure taken against the Russians, they had a counter measure. Any counter measure social media companies were using was "…being surpassed by foreign influence operatives, who adapt their tactics to either make their inauthenticity indiscernible, their automated propagation too rapid to control, or their operations compliant with terms of service."[9]

Russian tactics are becoming more challenging, and neither the public nor private sectors are able to keep up. "By design, Russian influence campaigns are multifaceted and designed to be deniable."[10] Early reports of the interference caused doubt in responses as "officials at all

levels of government debated whether publicly acknowledging this foreign activity was the right course. Some were deeply concerned that public warnings might promote the very impressions they were trying to dispel- that the voting systems were insecure."[11] As a result, the Russian's pitted the democratic freedoms and national security against each other, and Section 230 created a rigid dichotomy for the United States.

The Russian campaign has resulted in some changes in the private sector's willingness to take a more assertive approach, but the companies on their own are unlikely to adopt measures that risk fundamentally restricting freedom of speech. It has taken decades of domestic and international incidents for private companies to accept that one hundred percent free speech has severe consequences.[12] The mentality of the private sector has significantly evolved, however. Facebook's CEO, Mark Zuckerberg expressed, "I don't want anyone to use our tools to undermine democracy."[13] Previously, Twitter was the most unwilling of companies to regulate free speech, and expressed they are a "communication utility, not a mediator of content".[14] But as of 2019, Twitter announced that it would no longer authorize political advertisements when the investigations into the interference revealed how the Russians exploited their platform.[15]

It's apparent that Silicon Valley will continue to respond "just enough" to ensure they maintain their autonomy; however, they cannot guarantee their customers, the American electorate as well as Congress, full disclosure of what social media companies find or take action against. Americans across the spectrum are still reacting from the shock and awe of the scale in which the Russians were able to influence and manipulate American voters. It will take time for the whole nation to become literate in not only the internet of things (IoT), but the threat that operates within it. Until then, they are unlikely to blindly trust that these companies have taken measures to protect them.

A Closer Look at Influence Operations

Over the last couple of decades, the USG has placed a national priority on anti-insurgency and counter terrorism campaigns. As a result, many Americans have lost focus or have never witnessed Russian IO. The former Director of National Intelligence, James Clapper, argues that "Russian interference in the most recent US elections is not without precedent. The Soviet Union likely tried to influence *every* US election during the cold war."[16] However, many Americans are still unaware of what disinformation looks like or that they are used as pawns to advance foreign interests, and therefore requires an overview of what the Russian tactic and objectives are. It is also essential to understand the multi-dimensional nature of the concept of IO in order to appreciate the complexities of a solution. The need to protect the cognitive decisions made by the American electorate during elections is unprecedented, and the US needs a coherent strategy to address the threat.

Scholarship on IO reveals that there is ongoing debate among scholars and practitioners surrounding the definition of IO. Russia, as Peter Singer of *Like War* describes, "relied on clever manipulation and weaponization of falsehood called dezinformatsiya (disinformation) to gain the advantage over their enemies."[17] Its goal has been to "disrupt, damage, or modify what a target population 'knows' or thinks it knows about itself and the world around it."[18] The tactic is not only complex, and dynamic, but persistent. As a US Senate staff report, "Putin's Asymmetric Assault on Democracy in Russia and Europe," noted, "…the Kremlin's disinformation operations do not necessarily try to convince foreign audiences that the Russian point of view is the correct one. Rather, they seek to confuse and distort events that threaten Russia's image (including historical events), undercut international consensus on Russia's behavior at home and abroad, and present Russia as a responsible and indispensable global power."[19] Russia's goal

through use of IO is to push its national interests, whether in the US 2016 election, or its interventions in Syria, Ukraine, and other foreign arenas.

There is currently no official definition, or one agreed upon term for influence operations, but the US government has historically understood it as deception by use of propaganda or spreading disinformation. The USG describes Russian IO as *active measures*, *reflexive control* or *informatsionnoye protivoborstvo* (IPb). The US Military uses the term *information operations* as a tactical function of operations of the information environment (OIE); and researchers from RAND Corporation have introduced and explored the term *truth decay* in their published reports.[20] As of the 2016 election, then presidential candidate, Donald Trump, introduced the term "fake news" and unintentionally brought the attention of the IO threat to question. Multiple terms for disinformation contribute to the complexities, but despite consensus on one definition or term, scholars and practitioners agree the end state is to deceive in order to achieve political objectives. Hereafter, the term influence operations (IO) and disinformation will be used throughout this paper.

Additionally, researcher Buddhika Jayamaha, describes how Russian's, using the internet as a tool, operate under the framework of *Schismogenesis*, a term ancient Greeks coined to describe the intent of disrupting the public by creating division amongst citizens and political parties. Russia's goal is to delegitimize western democracy by influencing the US electoral process in order to shape the results of US elections for their own national interests.[21] Jayamaha describes the effects of "generating and intensifying hyper-partisanship on both sides of the political spectrum."[22] By creating this division, American voters look for extreme changes in policy, further sowing political instability that ultimately favors Russia's interests. A number of RAND reports on the study of truth decay depicted Russia's ability to cause disorder through

disinformation campaigns. The intent of delegitimizing democracy has affected decision making amongst government, military officials and American civilians.

Understanding the scope of Russia's influence efforts requires an appreciation of the variety of tools and methods Russia employs to achieve its ends. Russia tries to influence its targets through Information Related Capabilities (IRC) such as: psychological operations, electronic warfare, deception, and as of the last few decades, through cyberattacks into computer networks to execute a number of additional objectives. Technological tools and the development of the internet and social media has revolutionized the spread of disinformation. John Schindler, Author of "Obama Fails to Fight Putin's Propaganda Machine", reiterates that "there is nothing really new about this except how the internet gives propaganda unprecedented reach, quickly. [It] is merely an online version of the well-honed Cold War practice."[23]

The investigations into the 2016 elections revealed that Russia used several means to achieve their ends in undermining western democracy. Russians used a multi-prong approach to manipulate voters to push for extreme policy changes.[24] While many methods to defraud the United States knowingly violated US law and foreign policy, other methods, were unethical and malign, yet not illegal. The Russians used all legal tools provided.[25] Simply put, their tactics were "too new to be have clearly violated any existing laws."[26] The following section describes the methods that have been the most challenging for law makers and foreign policy advisors to respond to, starting with the actions led by another national leader.

The US Intelligence Community reported that Russia's president, Vladimir Putin, ordered the Internet Research Agency (IRA) to execute a pervasive influence campaign against U.S. voters using social media during the national presidential election. They established robust troll farms using information operators to spread disinformation through social media websites such

as Facebook, Twitter, YouTube, Instagram, and other common information sharing websites like Reddit. Operators known as "trolls" were able to conceal the locations of their Internet Protocol (IP) addresses by using virtual private networks (VPN); and they masked their identities by using fake social media accounts and stolen identities. Operators posted false information with doctored photos and fake articles with "clickbait titles, videos, and coordinated political rallies and protests. They used stolen private data to target voters of specific demographics in specific geographical locations, used bots to amplify their messages and flood news feeds with content, and committed espionage by soliciting real US persons to promote or disparage candidates.[27] Russian hackers broke into the Democratic National Committee and Hillary Clinton's campaign networks, and extracted critical information that Russian IO operators used against Hillary Clinton and her voters. IO efforts were not only limited to social media platforms, but also traditional news media such as Russian backed television networks like RT and radio channels such as "Sputnik"-- all with a wide line of influence to American citizens. "As of 2017, RT attracted about 22.5 million Facebook followers, and it deftly drives traffic to its platforms with human interest stories, cat videos, and pseudo conspiracy theories."[28]

The methods used in the 2016 election introduced a myriad of new means Russians to carry out against the US. Four major issues surfaced following investigations into the 2016 presidential election: 1) cyberattacks on voting infrastructure, 2) private data used for micro-targeting, 3) Russian funded political ads, and 4) the spread of disinformation and influence operations over traditional and social media. Each of these areas have been given priority and applied resources with the notable exception of number four.

"Moscow's campaign aimed at the US election reflected years of investment in its capabilities which Moscow has honed in the former Soviet states."[29] The success of the

campaign provided a proof of concept for the Russians.[30] By using old methods on more technologically advanced, but also vulnerable platforms, it has compounded the issues of Section 230. Though a partnership between the public and private sector has developed and some progress has been made to address Russian IO, a large part has been bifurcated. The culture and relationship between the public and private sector remain a barrier for forming a united solution. The internet and social media are increasingly becoming more important as sources of information for voters.

Key Stakeholders

This section identifies and analyzes the key stakeholders that will need to be part of any policy proposals. Understanding the positions, power, and interests of the key stakeholders helped shape this paper's recommended policy solutions, which addressed in the subsequent section. The three stakeholders significant to each policy alternative are: the private sector, the US Government and American citizens. Each stakeholder has a role in the balance of the polarity and inherently are in conflict with each other, but each has different goals, risk perceptions, and levels of influence.

The Private Sector

The top social media companies such as Facebook, Twitter, YouTube, Reddit and Instagram are the linchpin to countering Russian IO online, but they are stuck in a catch-22 situation. The collective goal of these companies is to offer a service that connects people, allows personal expression, and provides awareness of what occurs around the world. Since their creation, each company has advocated freedom of speech and expression to empower their users. They provide a platform for limitless global communication, but, as established above, also enable Russian objectives. Any amendment to Section 230 that would give the government

authority to implement security measures limits the private sector's capability and, in turn, risks their trust and relationship with customers. Restrictions also risk revenue, making companies less competitive in the market, which creates a conflict of interest and reluctance to hardening their platforms from nefarious foreign actors that contribute to that revenue. Prior to the elections these companies steadfastly resisted changes that would impact the status quo. Their willingness to make some incremental changes, moreover, appears designed only to give them a political buffer zone. Section 230 paved the path to the success social media companies have been able to achieve, and they will be loathe to entertain any real changes to the law. Ultimately, private companies "will have to decide whether they are prepared to sacrifice some autonomy in return for improved collective action."[31]

The U.S. Government

For more than 20 years, the USG has left Section 230 largely untouched. Even in the aftermath of Russian interference in the elections, the USG preferred other policy solutions. The USG holds the delicate role as the fulcrum that balances the polarity of freedom and security. Today, the USG is struggling with how to reposition the fulcrum when an imbalance occurs, while keeping careful consideration of both the interests of the private sector and American voters in mind. Upon learning of Russian hostile activity online, government leaders had a steep learning curve to understand the complexities of the digital threat. They initiated independent investigations and commissioned reports, held committee hearings, asked hard questions, established task forces, and crafted new policy in order to hold Russia responsible—actions that avoided attributing responsibility solely on Silicon Valley.

In its favor, the USG has experience in responding to these familiar cold war tactics. During the Cold War, the Reagan Administration introduced a whole-of-government approach

through the establishment of the Active Measures Working Group, under the Department of State (DOS), to identify and debunk the Soviet Union IO efforts.[32] This group would eventually evolve and take on other titles in an attempt to stay relevant through several presidential administrations. Following the Cold War, the Clinton administration eliminated the group. With the emergence of international terrorism and efforts to mend relationships with Russia, President Obama cancelled the Counter-disinformation Team. The DOS then established the Global Engagement Center (GEC), while both the Department of Homeland Security (DHS) and Federal Bureau of Investigations (FBI) committed their own IO support. Following the elections, the Counteracting Russian Hostilities Act of 2017 attempted to apply additional sanctions on Russia as a deterrent to future efforts to conduct an IO attack.

The USG has expanded many resources and attempted many different solutions in an effort to deter Russia's IO assaults, but it remains constrained by concerns that its efforts may tip the balance from freedom to security which may unintentionally provoke public opinion. Any feasible policy solutions will therefore require both the private and public sectors to reexamine the fundamental assumptions of national security.

The American Electorate

Both the private sector and the USG are in positions requiring them to tread lightly for fear of public dissent. The Edward Snowden scandal and speculation on illegal intelligence collection on US citizens bolstered longstanding concern by Americans over the idea of too much government oversight. The revelation of Cambridge Analytica's exploit and use personal data during the elections was also troubling to American social media users. Unless the private sector and USG can identify a resolution, the integrity of the electoral process lies in the hands of American voters who are otherwise unaware or unprepared for what they need to do to protect

themselves. Thankfully, the bridge between the private and public sector is not as wide as it may appear. By sharing a commonality in wanting to preserve freedoms and keep Americans safe, there is room for both entities to work together in the modern information domain in ways that can reassure the American public.

The American electorate is also an important stakeholder, of course, because it is the main target of Russian IO campaigns. "The Russian government spends an estimate 1.4 billion a year on disseminating its messaging through various media platforms"[33] In an effort to further divide American voters, these messages covered socially divisive topics such as the black and blue lives matter movements, immigration and anti-Muslim issues, gun laws, and anti-fracking campaigns to name a few. There were intelligence reports indicating that the Russians were shaping their messages to sway voters against presidential candidate, Hillary Clinton, and favor the Republican running candidate, Donald Trump. Other theories were that the Russians just wanted to undermine any candidate to incite anger over the entire democratic process and institution. The Russians, James Clapper expressed, were "hacking away at the very roots of our democracy."[34]

American's are the linchpin to the Russians achieving their objectives. Not only are they key targets, but they also sit between the crosshairs of the Russians, the private sector, and the USG. They are the customers, content creators and stakeholders of social media companies, and the constituents which government leaders serve. Any tip in the freedom-security balance affects not only the American electorate's freedom and security, but also the way they vote. The American people have a reasonable expectation that both the USG and private sector will keep them safe, but they also play a role in the management of the polarity as well. This is one of the challenges of Russian IO as social media users unknowingly enable the spread of Russian

disinformation and often times are unaware of what is occurring in the background. Potential drivers behind this are a lack of media literacy, limited awareness of Russian tactics, or biases towards or against socially divisive topics.

And the American public is a vulnerable target. In a Stanford University study that revealed 80 percent of students were unable to identify credible sources, academic professionals noticed the increasing need for media literacy.[35] A PEW research study revealed that seven out of ten American's use social media. Facebook is the second leading social media company with 69% of Americans as users, of which 74% log-on daily.[36] "With the exception of YouTube – the video-sharing platform is used by 73% of adults – no other major social media platform comes close to Facebook in terms of usage."[37] There is a large population of Americans who are of voting age and susceptible to sharing disinformation or believe the disinformation to be true. Fortunately, after the wide attention given the Russian interference following the 2016 election, many Americans are more informed of the risk; but without social media or government intervention, awareness and media literacy is the first line of defense, and for now, the only line of defense. As future national elections approach, American voters will need to be more knowledgeable on how Russians exploit them and he medium they use to inform their vote.

Identification of Policy Alternatives

Any policy solution—and this paper explores three primary alternatives—will need to balance the polarity of freedom and security; protecting the very openness required for American democracy's functioning with the risks such as openness poses in abetting foreign interference. A basic premise of any solution is that it is not a question of *if* the Russians will conduct an IO attack, but when. Certainly, there is no shortage of regulations the USG can enforce upon the private sector that could deny the Russian's ability to exploit American voters through social

media platforms. However, such a one-sided security approach would cause a drastic imbalance in the polarity. The democratic institution would reject any approach that completely denies the Russian threat; therefore, a strategy must have a framework that can cyclically detect, deter and defend against the threat, shifting nimbly from security to openness in ways that shield *and* maintain democracy. All stakeholders have a part in achieving each objective.

The main component to detecting Russian disinformation or influence operations is collaboration through information sharing among the private and public sector and educating the public to enable further detection. The continuing effort of this objective along with a massive awareness campaign will aid in accomplishing the second and third strategic objectives to defend and deter. "Awareness is perhaps the single most important defense against such interference and an essential tool toward building a resilient democracy."[38] The intent of this campaign is to minimize the effects that IO has on the population and thus exhausting Russian resources and invoking a sense that their efforts do not achieve the return on their efforts. Detection and defense are critical to achieving deterrence.

In this section, three policy alternatives are examined and assessed to determine the best strategy that can be used to achieve these objectives. The first alternative examines the status quo. The second alternative is an adjustment to Section 230 of the 1996 Common Decency Act. The third and final alternative is expanding the DOS Global Engagement Center to lead a private/public partnership and awareness campaign.

Alternative One – The Status Quo

This option continues the status quo between the USG and the private sector. The social media web owners can decide for themselves the best options for their customers, and the USG can take its own measures to protect the public. It requires no amendments to Section 230, which

eliminates the concern of government control or oversight and permits private companies the liberty to institute their own methods to detect, defend, deter or even completely deny Russian activity. Employing a deniable measure such as secretly blocking Russian access, should a private company choose to use that method, would be their prerogative. Such a measure is unlikely, however, given the private sector's incentives, as outlined above.

Since the 2016 election, the private sector instituted several changes to protect their customers. They also introduced revolutionary methods such as artificial intelligence (AI) to help respond to evolving Russian IO tactics and techniques. By maintaining the status quo, the current changes and measures, the government would need to assess the effectiveness in the runup to the 2020 election, relying on both the public and private sector will need more research to determine how and if Russian techniques have changed to surmount any status quo solution.

Alternative Two- Section 230 Reform

Alternative two adjusts Section 230 of the 1996 Common Decency Act commensurate with the present and emerging digital threats on social media platforms. The intent of this adjustment is to hold the private sector accountable for the role they play in amplifying disinformation. It serves as a forcing function for the private sector to take more action, balancing the revenue incentives that currently drive private sector behavior. This adjustment would require social media companies to monitor and remove content posted online known to be disinformation or other identifiable Russian IO activity. It also would require that they provide awareness to their customers on all detected activity to include known fallacies of shared information. Exposing Russian tactics and threat trends will enable customers to take pause before sharing content and further spreading disinformation.

This alternative facilitates improved collective action amongst the public and private sectors. Updating Section 230 allows the companies to meet the present security needs by preserving their autonomy to decide how they execute those security measures. The USG is aware of the concerns this adjustment would have on freedom of speech and potentially forcing companies to take draconian action. Changes to Section 230 would include a fine on companies that do not comply with Section 230, but it would also provide a level of amnesty for companies that take proactive measures to detect and defend against the threat.

Alternative Three – Expand the Global Engagement Center (GEC)

The third alternative seeks a more collegial approach through expanding the DOS' Global Engagement Center authorities to include a heavy private partnership that fosters collaboration on risk management and achieves solutions in concert. Expanding a program under the DOS leverages the experiences from both the public and private sectors and dedicates assets and resources towards the threat of Russian IO. It also allows them to navigate the threat together, while crafting solutions such as creating a strategic, non-partisan awareness campaign. Having a private public enterprise fall under this department allows a seamless stream of support from the intelligence community and having the right resources from both sides of the aisle to react as needed, multiplies the GEC's effectiveness. The intent of this partnership is to provide a forum of open dialogue and information sharing between the two sectors to create a common understanding of the threat and a united effort in tackling the dysfunction it creates by making it less likely to impact the choices voters make.

The Global Engagement Center (GEC), originally established to counter Islamic terrorist recruiting efforts, transitioned to countering foreign disinformation. The GEC attempts to achieve their objectives through governmental interagency participation from the intelligence

agencies, DHS and the Department of Justice (DOJ). The GEC is the only combined public effort that focuses on foreign IO; however, program budget cuts have limited the capability, resulting in bifurcated efforts even amongst the government.[39] A government-only approach will not survive or be successful without including the private sector. Sharing observed Russian malign activity from the view of social media companies allows the government to support and dedicate resources. Private industry has been reluctant to share cybersecurity intrusions for fear of it impacting revenue; however, making the public sector aware of activity that occurs on publicly accessible websites is not associated with the same risks. To incentivize information sharing, this commission will authorize grants to companies that reveal information that contribute to tangible prevention efforts.

Evaluation Criteria and Analysis

Five evaluation criteria were selected and weighted to help differentiate among the alternatives that would best aid in balancing the security-freedom polarity: 1) performance, 2) time, 3) risk, 4) feasibility, and 5) cost. Each alternative received a score on a scale of one to five, with the highest score reflecting the most successful option. Performance and feasibility aim to achieve a high score based on the ability to meet objectives and achieve maximum cooperation with minimal political and private opposition. Though each alternative favors a low amount of time, risk, and cost to achieve their objectives, a high evaluation score is favorable based on each alternative's ability to reduce the amount of time, risk and cost through planning and execution.

- **Performance** is evaluated on the ability of an alternative to achieve the best balance in the security-freedom polarity and accomplish the strategic objectives of

detect, defend and deter against Russian IO. Performance is the most critical criterion and therefore is weighted the highest criterion at 5.

- **Time** is evaluated by how long it would take to implement an alternative as well as the length of time it would take to achieve the strategic objectives. With reoccurring annual elections, time is the second highest weighted criterion with a weight of 4.
- **Risk** is assessed on the likeliness of unintended shifts in the polarity balance and is given the weight of 3.
- **Feasibility** is assessed in the ability to achieve private sector cooperation as well as achieving political will associated with each alternative. It is also weighted at 3.
- **Cost** is evaluated based on the monetary expense of implementing an alternative and is weighted at 2.

The table below reflects the results of how each alternative was measured against the selected weighted criteria. An analysis of the scores will be provided in the next section.

Analysis of Alternatives

The analysis of alternatives is summarized in the following decision support matrix.

	Criteria					
CRITERIA DESCRIPTION	**Performance (5)**	**Time (4)**	**Risk(3)**	**Feasibility (3)**	**Cost (2)**	
WEIGHT	5	4	3	3	2	
	29%	24%	18%	18%	12%	
Alternatives	**Criteria Scores**					
Alternative 1: Status Quo	2 (10)	3 (12)	2 (6)	2 (6)	3 (6)	12 (40)
Alternative 2: Adjust Section 230 Awareness Campaign	4 (20)	3 (12)	2 (6)	3 (9)	2 (4)	14 (51)
Alternative 3: GEC-Public/Private Apprach	5 (25)	2 (8)	5 (15)	4 (12)	3 (6)	19 (66)

Performance

Performance is an important criterion because each alternative's level of performance determines the effect a solution has in maintaining the balance of security and freedom while accomplishing one of the three strategic objectives: deter, detect and defend. Although some changes were made by individual companies within the private sector, maintaining the status quo does not guarantee the private sector collectively matches the same measures. This option allows the private sector to implement their own changes as they see fit, but many customers of one social media platform are simultaneously users of others. The same threats exist across the information sharing websites. The status quo not only enables a bifurcated effort amongst the private sectors, but it maintains the divergent approach to the balance of security and freedom, therefore a balance is not achieved with this option.

Alternative 2 rates marginally higher in performance as the adjustment to Section 230 will enforce more involvement from the private sector in providing security measures, measures that meet the strategic objectives. Though this option gives the private sector the autonomy to

choose what and how to implement security measures and provide awareness to their customers, it is not an alternative that achieves a complete even balance. If meeting the objectives to deter, detect and defend against Russian IO was the only performance measure and defined success, then this alternative would be suitable. However, forcing the private sectors hand while holding them accountable for all the content on their sites does not lend to a balance of freedom and security.

Alternative 3, the GEC public-private partnership approach, rated the highest in performance as a result of its ability to collectively achieve the strategic objectives commensurate with the freedoms of the private sector. Though the private sector is required to join the public in a joint effort, the joint collaboration offers the opportunity for them to share the best approach in providing awareness on their individual platforms and negotiate variances that best fit their interface.

Time

Time is a heavily weighted criteria due to the concerns about the rampant use of IO during reoccurring elections, with the House of Representative elections every two years, and presidential elections every four years, amid a flurry of local and state elections. Though it takes time for two of the alternative solutions to be put in place and meeting the identified objectives will be enduring, some alternatives provide more timely options than others. In this case, Alternative one, the status quo, obviously rated the highest of the three due to the continuation of the current state of affairs. However, it still only received a medium rating of three due to the amount of time it takes the government to emplace measures as a result of operating separately from the private sector. Working together would cut time down significantly, but not immediately. Alternative two scored similarly as it would still take time to pass legislation while

anticipating appeals from the private sector. Alternative three scored the lowest, although implementing a joint center would not take a large amount of time to standup, cutting through cultural barriers would.

Risk

Risk is a critical criterion to consider for each alternative to avoid tipping the balance of the freedom-security polarity unfavorably in one direction or another. Alternative one rated low due to the balance shifting unfavorably for security. While the private sector made some changes, others still cause the spread of disinformation and the use of IO. Alternative two, shifted the balance too far in favor of security and could cause unintended consequences at the cost of freedoms of speech online. Though Section 230 would put protective measures in place for web companies that made visible efforts to remove disinformation, it could not guarantee that it would not force companies to put severe measures in place to protect themselves from fines. This could drive customers away, hurting their business entirely. Alternative three scores the highest again as collective action mitigates the most risk to a shift in balance.

Feasibility

Feasibility is a criterion essential in evaluating the challenges of limited political will and private opposition each alternative would face. Evaluating the feasibility can determine the long-range success of an alternative through the support and cooperation of stakeholders. Solutions to manage the freedom-security balance are contentious, but the three alternatives face a catch-22 dilemma. Alternative one received a low rating as a result of marginal change despite more change desired from the majority of the public sector and American electorates. Alternative two only scored slightly better due to the concerns of too much change by the private sector and a part of the public sector that opposes changing Section 230. The government can expect that the

private sector, despite their interests to protect their customers, will fight aggressively to ensure their full autonomy. Alternative three scored the highest as the GEC offers the best avenue to receive support in that it offers mutually favorable collective action.

Cost

Cost, similar to time, is exhausted more when security measures are emplaced independent from one another. Alternative one received a medium rating due to the expense incurred by the government to put measures in place that could be alleviated by a private sector that already has the resources to execute. Alternative two rates low, as expenses for private companies would increase in order to facilitate the surge in monitoring and removing IO related content. Cost is sure to rise as private sectors will pay expensive legal fees to fight changes to Section 230. Alternative three received a medium rating for the low expense required to plan for and stand up a joint engagement center.

Recommended Approach

Based on the analysis and results from the decision matrix, alternative three, Expand the GEC to host a public-private collaboration and awareness campaign, received the highest rating and is the strongest solution to maintain the balance of freedom and security. Alternative three received an overall weighted score of 66, fifteen points ahead of Alternative two which rated at 51, eleven points above alternative one. Though alternative three scored moderately lower under the time criterion compared to alternatives one and two, it scored the highest in performance and had the lowest risk of the three. The provided analysis and associated ratings echo that the opportunity for the private and public sector to combine efforts is the most appropriate solution.

Developing solutions necessitates joint collaboration because of the ability to combine information, talent and diverse experiences. Both the public and private sector respectively have

different views and methods of observing and collecting information on their networks and different ways of responding to Russian activity. They also each have their own operators with different cyber qualifications and experiences as well as top-notch researchers. Though they have their differences, as well as their unique limitations and constraints, combining cutting-edge technology and sharing information allows the government to provide the best solution.

Beyond these practical benefits, by its nature joint collaboration ensures an organic, living balance among competing interests and priorities, as the different players work together in a collaborative process that can achieve the strategic objectives in the detection, defense and deterrence of Russian disinformation online.

Implementation Plan

In order to be successful, a joint collaboration under the GEC will require a strategic plan that can stand the test of time and adapt with evolving technology, dynamic threats, and multiple presidential administrations. Expanding the GEC should not encounter any large impediments; but once restructured, navigating through cultural barriers, building mutual trust, developing roles of responsibilities, and negotiating memorandums of agreements will be anticipated impediments. This section walks through the strategy to implementation of the newly designed center. It will also provide a force field analysis on both assets that will empower the GEC and uncover additional impediments that could thwart operations. The Implementation plan for alternative three includes four phases. Phase one is to conduct shaping operations, develop a concept plan and establish standard operating procedures and agreements among the USG and private industry. Phase two is to build the team and recruit from within the government and private firms, industry, and academia. Phase three includes the development of a logic model to facilitate development of activities, objectives, and goals for the program, and phase four

includes the development of program evaluation criteria. The remainder of this section will walk through each phase.

Phase one includes establishing the new GEC by initiating a small think tank in the interim that will be led by DOS. The organization will be comprised of public and private members as well as members from industry and academia. Public members will include representatives from the DHS, DOJ, DOS and other members from the intelligence community (IC). Private members will consist of researchers and engineers from Facebook, Twitter, Reddit, Snapchat and Google, who are the parent owners of YouTube. Members from academia and industry will provide consulting on structural and organizational approaches to ensure the GEC achieves optimal success. Starting as a small think tank will allow for control of the integration and implementation of ideas for the mission of the center. The conclusion of this phase will be determined when both the public and private sector have approved and agreed to all SOPs and MOAs that outline the roles and responsibilities of the GEC.

The second phase is to champion GEC integration by converging the rest of the public and private sector team members, but also recruiting and hiring from the outside to include engineers, analysts, and fact checkers from industry and academia. This phase will focus on developing and training the workforce and leadership while cementing a new joint operational culture. Growing the center with an established backbone will allow the organization to expand and execute its mission in a unified effort.

Phase three will further develop the concept plan by envisioning the centers objectives through the next 2024 presidential election and will build the organizational structure to reflect the resources and expertise needed to be successful. They will develop the GEC's mission, vision, lines of effort and strategic objectives. Clearly defining the lines of effort and objectives

is key to integrating capabilities across the organization together with joint partners and collection capabilities. The GEC's lines of effort include three strategic objectives: detect, defend and deter IO activity on the social media platforms. The main component to the first strategic objective will be information sharing amongst the private and public sector to detect all Russian disinformation. This will be enabled by building an intelligence collection plan that both entities can use to collect and answer critical information requirements.

A force field analysis is mostly required for this phase of the implementation plan as it has the most anticipated obstacles. Like expanding many organizations, getting through the cultural barriers brought from previous operating environments and building mutual trust will be the largest and most strategic barrier to overcome. Time will be the largest impediment as it takes time to work through growing pains of establishing new organizations. However, a joint effort facilitates an open environment that allows the freedom to offer ideas and approaches used to tackle a shared problem set. Achieving mutual trust will be possible because it is no longer just a private or public problem to overcome, but now a collective team problem.

Finally, the fourth phase includes identifying program evaluation criteria to assess the center's ability to achieve their objectives. Assessing the outcomes of this approach will take time to measure, and time is an impediment that cannot always be avoided; however, structuring the GEC to operate and adapt to new tactics, with the right partners allows for immediate progression with minimal impacts to the freedom-security balance. In the interim, giving freedom of maneuver to both public and private leaders is a significant improvement to the impediments they first faced during the 2016 presidential election. Employing this alternative approach provides a framework that can improve and sustain a whole-of-nation response when the US democratic institution and national security is threatened.

Conclusion

The Russian interference in the 2016 presidential election is, in no small part, due to both the public and private sectors not sharing enough information—and trust—with one another and with the public. The collective reticent behavior was telling of the public-private partnership and resulted in intelligence failures from both sides of the aisle. "[Russian] activities started as early as 2014, but its existence and activities were not well known to the wider American public and the US Government until well after the election had passed."[40]

The handling of the Russian threat compounded with previous disclosures of intelligence and data gathering on Americans, has generated distrust for the public and private sectors amongst American citizens. Although both sectors experienced the fallout from those events, the election shed further light on the strained relationship, and raised concerns about the ability of either to constructively respond to threats. If either the public or private sectors believed they could operate without each other's intelligence, they are sorely mistaken. A joint effort not only allows for constructive solutions but can restore full faith and trust into both institutions.

To be successful, the public nor private sectors can compartmentalize information and there cannot be divergent values amongst the two sectors. The values of freedom and security should be the two guiding principles when creating a vision and lines of effort. One line of effort for this alternative is bringing awareness to the American electorate through public references on official government websites and social media platforms. Currently, the DHS and FBI offer helpful online resources and warnings to voters; however, they are out of the line of sight for those who predominately or solely use social media. Sharing information provides an opportunity to bring awareness through a social media platform and trusted official government

websites. Speaking with one voice instills trust; and bringing awareness is the greatest defense method that can possibly deter, detect and defend against the Russians online.

The case study of the 2016 presidential election and the Russian reemergence and persistent use of disinformation on social media presents a polarity of freedom and security. The divergence amongst the two along with other issues of trust in the government and threats of censorship remains a sensitive domestic issue following the 2020 presidential election. Russian interference still poses a significant threat to US democratic institutions and to US national security that the USG and tech companies must address. All the forementioned events serve as a clarion call for a solution that can restore faith for Americans into government and private institutions, strengthen the public-private relationship and rebalance the polarity while also mitigating the Russian threat.

A study into the uses and tactics of influence operations reveals how it exploits US freedoms and security and the impacts it can have if the US fails to respond. The government has a responsibility to provide for the welfare of all its people, but private social media companies want to ensure the preservation of freedom of speech for all users on their platforms.

As this paper is written in 2021, the pandemic of the novel COVID-19 virus reflects how easily misinformation can spread worldwide, but it also presents how disinformation will increase in order to amplify already chaotic moments such as a global pandemic or the rise in domestic terrorism, as seen in the January 2021 insurrection at the Capitol. The COVID response has been marked by collaborative efforts by the government and all of society similar to the approach analyzed in the policy alternative above. Social media companies like Facebook's "COVID19 Information Center" and Twitter's, "COVID19 Top Stories" were established to provide the latest updates and prevention tips. One silver lining presented from the response to

the pandemic is that a joint effort to confront a challenge for a nation can be achieved through mutual respect and rigor. Social media companies were paramount in helping spread awareness of the virus; and the cooperation from society will, in no small part, reflect how those efforts fare. Their response has been a proof of concept in how joining together and collaborating to provide awareness and accurate information is possible. When the pandemic has subsided, the public and private sector along with the electorate can reflect on the actions that benefited society as a whole. The successes from the pandemic response should be adopted by the government as it looks as far afield to prepare for 2024 and beyond. Identifying a solution when political emotions are low, and cognition is high, will result in a stronger whole-of-society response to Russian influence operations and securing the American electoral process.

[1] Singer, *LikeWar*, 264.
[2] Valariano, Brandon, "International Relations Theory and Cyber Security", 259.
[3] Singer, *LikeWar*, 16.
[4] Stengel, *Information Wars,* 294.
[5] Singer, *LikeWar,* 224.
[6] Stengel, *Information Wars,* 295.
[7] Selyukh, Alina, "Section 230: A Key Legal Shield for Facebook, Google Is About to Change."
[8] Balakrishnan, "Anita, Facebook pledges to double its 10,000-person safety and security staff by end of 2018."
[9] Senate.gov, "Russian Active Measures Campaign and Interference in the 2016 U.S. Election, Vol 2," 75.
[10] DNI.gov, Background to "Assessing Russian Activities and Intentions in Recent US Elections," 2.
[11] Senate.gov, "Russian Active Measure Campaign and Interference in the 2016 Election, Vol I," 4.
[12] Singer, *LikeWar,* 241.
[13] Singer, *LikeWar,* 241.
[14] Singer, *LikeWar,* 229.
[15] Conger, "Twitter Will Ban All Political Ads, C.E.O. Jack Dorsey Says."
[16] Clapper, *Facts and Fears,* 314.
[17] Singer, *LikeWar*, 103.
[18] Singer, *LikeWar,* 183.
[19] Senate Minority Staff Report, "Putin's Asymmetric Assault on Democracy in Russia and Europe," 39.
[20] Kavanaugh, *Exploring Media Literacy Education as a Tool for Mitigating Truth Decay.*
[21] Jayamaha, *Social Media Warriors: Leveraging a New Battlespace.*
[22] Jayamaha, *Social Media Warriors: Leveraging a New Battlespace.*
[23] Schindler *Obama Fails to Fight Putin's Propaganda Machine.*
[24] Senate.gov, "Russian Active Measure Campaign and Interference in the 2016 Election," Vol I, 17.
[25] Stengel, *Information Wars,* 292.
[26] Singer, *LikeWar,* 298.
[27] Hickey, "Election Interference: Ensuring Law Enforcement is Equipped to Target Those Seeing to Do Harm."
[28] Senate Minority Report, "Putin's Asymmetric Assault on Democracy in Russia and Europe," 41.

[29] DNI report, "Assessing Russian Activities and Intentions in Recent US Elections," 2.
[30] Singer, *LikeWar,* 26.
[31] Haass, "World Order 2.0, The Case for Sovereign Obligation," 9.
[32] Schindler, "Obama Fails to Fight Putin's Propaganda Machine."
[33] Huguet, "Exploring Media Literacy Education as a Tool for Mitigating Truth Decay."
[34] Clapper, *Facts and Fears,* 314.
[35] Huguet, "Exploring Media Literacy Education as a Tool for Mitigating Truth Decay."
[36] Perrin, "Share of U.S. Adults using social media, including Facebook, is mostly unchanged since 2018."
[37] Perrin, "Share of U.S. Adults using social media, including Facebook, is mostly unchanged since 2018."
[38] Corn, "How to Stop Russia From Attacking an and Influencing the 2020 Election."
[39] Gramer, "State Department Ramps up War Against Foreign Propaganda."
[40] Senate.gov, "Russian Active Measures Campaign and Interference in the 2016 U.S. Election, Vol 2," 75.

Bibliography

Balakrishnan, Anita. “Facebook pledges to double its 10,000-person safety and security staff by end of 2018.” https://www.cnbc.com/2017/10/31/facebook-senate-testimony-doubling-security-group-to-20000-in-2018.html.

Clapper, James and Trey Brown. “Facts and Fears.” Viking Press, 2018.

Conger, Kate. “Twitter Will Ban All Political Ads, C.E.O. Jack Dorsey Says.” https://www.nytimes.com/2019/10/30/technology/twitter-political-ads-ban.html.

Corn, David. “How to Stop Russia From Attacking an and Influencing the 2020 Election.” https://www.motherjones.com/politics/2019/09/how-to-stop-russia-from-attacking-and-influencing-the-2020-election/.

DNI.gov, Background to “Assessing Russian Activities and Intentions in Recent US Elections,” 2. https://www.dni.gov/files/documents/ICA_2017_01.pdf.

Gramer, Robbie and Ellias Groll. “With New Appointment, State Department Ramps up War Against Foreign Propaganda.” https://foreignpolicy.com/2019/02/07/with-new-appointment-state-department-ramps-up-war-against-foreign-propaganda/.

Haass, Richard. “World Order 2.0, The Case for Sovereign Obligation,” Vol 96, Number 1, Jan 2017 Foreign Affairs. https://www.foreignaffairs.com/articles/2016-12-12/world-order-20.

Hickey, Adams. “Testimony before Senate Judiciary Committee: “Election Interference: Ensuring Law Enforcement is Equipped to Target Those Seeing to Do Harm.” https://www.justice.gov/opa/speech/deputy-assistant-attorney-general-adam-s-hickey-testifies-senate-judiciary-committee.

Huguet, Alice, Jennifer Kavanagh, Garrett Baker, and Marjory S. Blumenthal. “Exploring Media Literacy Education as a Tool for Mitigating Truth Decay.” *RAND Corporation*, (2019). https://www.rand.org/pubs/research_reports/RR3050.html.

Jayamaha, Buddhika, Jahara Matisek. "Social Media Warriors: Leveraging a New Battlespace." *Parameters* 48, no. 4 2019: 11-23. https://search.proquest.com/docview/2261275477?accountid=11091.

Johnson, Mica. "Fighting “Fake News": How We Overhauled Our Website Evaluation Lessons." *Knowledge Quest* 47, no. 1 2018: 32-36. https://search.proquest.com/docview/2101237228?accountid=11091.

Kavanagh, Jennifer and Michael D. Rich. "Truth Decay: An Initial Exploration of the Diminishing Role of Facts and Analysis in American Public Life." *RAND Corporation,* 2018. https://www.rand.org/pubs/research_reports/RR2314.html.

Perrin, Andrew and Monica Anderson. "Share of U.S. Adults using social media, including Facebook, is mostly unchanged since 2018." https://www.pewresearch.org/fact-tank/2019/04/10/share-of-u-s-adults-using-social-media-including-facebook-is-mostly-unchanged-since-2018/.

Schindler, John. "Obama Fails to Fight Putin's Propaganda Machine." https://observer.com/2015/11/obama-fails-to-fight-putins-propaganda-machine/.

Selyukh, Alina. "Section 230: A Key Legal Shield for Facebook, Google Is About to Change." https://www.npr.org/sections/alltechconsidered/2018/03/21/591622450/section-230-a-key-legal-shield-for-facebook-google-is-about-to-change.

Senate Minority Staff Report, "Putin's Asymmetric Assault on Democracy in Russia and Europe," 39. https://www.foreign.senate.gov/imo/media/doc/FinalRR.pdf.

Singer, P. W., and Emerson T. Brooking. "*Like War: The Weaponization of Social Media.*" New York, NY: Houghton Mifflin Harcourt, 2018.

Stengel, Richard. *Information Wars: How We Lost the Global Battle Against Disinformation & What We Can Do About it.* New York: Atlantic Monthly, 2019.

Valariano, Brandon and Ryan Maness. "International Relations Theory and Cyber Security: *Threat, Conflict, and Ethics in an Emergent Domain*", 259. http://www.brandonvaleriano.com/uploads/8/1/7/3/81735138/international_political_theory_and_cyber_security_-_oxford_handbook_valeriano_and_maness_2018.pdf.

U.S. Congress. Senate. Subcommittee on Cybersecurity; Committee on Armed Services Senate. *Cyber-Enabled Information Operations*. 115th Cong., 1st sess., 2017. https://congressional.proquest.com/congressional/docview/t29.d30.hrg-2017-ash-19884?accountid=11091.

U.S. Congress. Senate. Select Committee on Intelligence; United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election Volume 1: Russian Efforts Against Election Infrastructure. 116th Cong., 1st sess., 2017. Accessed January 18, 2020. https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf.

U.S. Congress. Senate. Select Committee on Intelligence; United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election Volume 2: Russia's Use of Social Media. 116th Cong., 1st sess., 2017. https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf.